This is a peer-reviewed, accepted author manuscript of the following research article: Wright, J 2025, 'Does Scotland's green energy strategy improve security of North Sea critical national infrastructure?', *Scottish Affairs*, vol. 34, no. 1, pp. 70-92. https://doi.org/10.3366/scot.2025.0535

Does Scotland's Green Energy Strategy Improve Security of North Sea Critical National Infrastructure?

Abstract

Scotland's natural endowment makes it an extremely effective location for renewable energy generation. The 'green' transition needs to be managed carefully to ensure that energy provision remains resilient across all sectors, benefits communities and supports local economic development. Rising threats to the energy sector pose additional significant risks to this transition. As Scotland pursues its goal of becoming a net zero economy and trailblazer in renewable energy, greater attention must be given to the cyber-physical security of its interconnected maritime structures. Without such consideration, the remainder of the supply chain may be left vulnerable to attack, with potential catastrophic consequences.

This opinion piece explores the challenges and opportunities Scotland could encounter in safeguarding cyber-physical maritime infrastructure, drawing insights from a comprehensive literature review of recent studies, articles and reports. The article explores the conceptual frameworks of resilience, security and critical national infrastructure, analyses the current maritime security landscape and assesses Scotland's capacity to ensure effective critical infrastructure security measures are put in place. Through this analysis, the article aims to provide a balanced perspective on the effectiveness of current security measures within the context of evolving threats and devolution. The article concludes that there is an opportunity for Scotland to champion innovation, progress infrastructure security and foster greater cohesion across UK government departments.

Keywords: cyber security, critical national infrastructure, maritime security, energy infrastructure, resilience, cyber-physical systems

Introduction

In January 2023, the Scottish Government published the draft ‘Energy Strategy and Just Transition Plan’ articulating the roadmap and ambitions for Scotland’s Energy sector. In line with commitments made at the 26th United Nation Climate Change Conference of the Parties (COP26), this strategy aims to highlight Scotland’s commitment to leading the way in renewable energy and to ensure an inclusive transition to a low-carbon economy (Scottish Government, 2023). However, following a report from the UK Climate Change Committee, Scotland has retracted its 2030 target of reducing gas emissions by 75 per cent. This marks the eighth target missed in the past 12 years, and is the result of an "insufficient delivery" plan and inadequate progress (Kerr, 2024; Climate Change Committee, 2024).

Scotland has a history of concern for climate change. The Scottish Government were first to legislate climate action, with the 2009 Climate Change Act, and was the first to declare a global climate emergency in 2019 (Cunningham, 2019; WWF, 2021). Therefore, it is unsurprising that Scotland aspires to set the standard for climate action by investing in North Sea renewable energy infrastructure. While this ambition is laudable, it requires a balanced approach with thorough consideration of the costs, benefits and overall outcomes.

Home to circa 800 islands and 16,500km of coastline, Scotland is advantageously positioned to utilise its abundance of wave and tidal resources for energy production (Fig.1). The establishment of the world leading European Marine Energy Centre (EMEC) in Orkney (2003) underlined this position (EMEC, 2024). Currently, 25% of Europe’s offshore wind power and tidal energy is generated by Scotland. There is also potential to harness around 10% of wave energy (Gray, 2023). One of the world’s largest tidal turbine collections is located between Scotland’s mainland and the Island of Stroma, illustrating Scotland’s expertise. It generates energy from tidal currents between the Atlantic Ocean and the North Sea and, in 2019, powered almost 4,000 homes (Edmond, 2020). The Draft Strategy looks to build on this success and the commitments made in the Bute House Agreement to achieve:

- 8-10GW of additional renewable energy capacity by 2030;
- Greater support for the growth of marine renewables and the offshore wind sectors;
- A vision for solar energy;
- A strengthened heat in buildings policy framework; and
- A 10-year Just Transition Fund totalling £500 million to support projects contributing towards net zero (Scottish Government, 2023).

[Figure 1]

Collaboration between countries neighbouring the North Sea is vital to achieve Scotland's ambitions. The North Sea has been coined the 'battery for Europe', making it strategically advantageous to embark on a shared mission. This would facilitate the creation of mutually beneficial and tested innovations that harness energy potential and create supply security (Neal & Bueger, 2023). Scotland has partnered with wind energy market leader, Denmark, to share knowledge and collaborate on energy projects, and has broadly increased engagement across the Nordic and Baltic regions (Scottish Government, 2017). Thus, enhancing economic and trading opportunities, accelerating the green transition through shared expertise, and bolstering the government's ability to advocate for common interests and values on the global stage (Scottish Government, 2022). This presents manufacturers with the most significant growth opportunity anticipated in the next 20 years (Scottish Enterprise, n.d.).

Energy projects all require subsea electricity connections and an increasing number of cables connecting national grids to the European energy market. These connections are vital for global data traffic and energy supply but are inherently vulnerable to accidental and deliberate damage – a principal concern of the North Atlantic Treaty Organisation (NATO) (McNamara, 2024). In recent years, Russian activity within the North Sea has escalated. Nordic intelligence reports claim that Russian ships are mapping windfarms and communication cables (Connolly, 2023). Historically, Russia has had a pivotal

foothold in the energy market. However, the ‘green’ transition reduces reliance on Russian fuel. This has led to Russia using energy as a foreign policy tool, whereby those who buy Russian oil are rewarded (‘petro-carrots’), and those who do not are harshly punished (‘petro-sticks’) (Newnham, 2011). Along with the Nord Stream pipeline attacks in the Baltic Sea, these growing energy threats have highlighted the strategic importance of maritime critical infrastructure (Neal & Bueger, 2023). This everchanging risk of international attack demands far greater collaborative efforts directed towards protecting new North Sea energy developments. Whilst NATO have commenced this effort with the establishment of a new Critical Undersea Infrastructure Network, enhancing the security of energy infrastructure requires a holistic approach across government and within industry (NATO, 2024).

This paper will endeavour to answer the question: ‘Does Scotland's Green Energy Strategy improve security of North Sea Critical National Infrastructure?’

Defining CNI, Security and Resilience

To answer this question, definitions for “critical national infrastructure”, “security” and “resilience” need to be delineated.

Critical National Infrastructure

NATO defined “national infrastructure” as: *“Installations which are set up for the maintenance and training of national forces in time of peace, and for the defence of the homeland in time of war”* in the early 1950s (Ismay, 2001). This definition referenced key physical points within a nation’s infrastructure likely to be targeted by hostile actors (Tyrrell, 2001). Nowadays, the term is used in policy discussions concerning infrastructures (or systems) deemed necessary for the effective function of a state. In the UK, consideration for national infrastructure commenced in the late 1990s with the establishment of the National Infrastructure Security Co-ordination Centre (NISCC) in 1999 (NISCC, 2004). However, the first UK public policy document to incorporate the term was not published until 2010 and failed to provide a formal definition (HM Treasury, 2010).

Changes in the global threat landscape, brought into focus by the 9/11 terror attacks, highlighted a knowledge gap regarding infrastructure dependencies and the imperative for safeguarding them (Steola, *et al.*, 2016). Security and protection of national infrastructure has since become a primary concern on the global agenda (Rees and Rees, 2023). This concept has evolved into “critical national infrastructure” (CNI) (Fig.2).

Worldwide, countries have proposed different definitions for the “critical” aspect of national infrastructure (Table 1) and have identified different CNI sectors (Table 2). Whilst this creates a necessity to define the system, asset or service of concern, “critical” infrastructure can be described as essential for economic and societal well-being, public protection, and the operation of key government duties, without which “catastrophic and far-reaching damage” would ensue (OECD, 2008).

As Scotland is a UK nation, this paper will use the UK definition of CNI. Only certain CNI assets fall under Scotland’s jurisdiction in line with devolved or partially devolved agreements with the UK Government. Further analysis of the implication of devolution on CNI will be provided later.

[Table 1]

[Table 2]

Security

Throughout history, the concept of security has evolved according to the political and economic landscape of a nation. In its broadest sense, security is defined subjectively as “an absence of fear” (Osgood, 1954). However, current politics has ‘expanded’ the definition of security: from the “security of nations to the security of groups, individuals [and the physical environment]”; from “military to political, economic, social, environmental, [technological, and] human security”; and from nation-state security to security of international institutions, local governments, and non-governmental organisations (Brooks, 2010; Rothschild, 1995).

The multidimensional nature and diverse application of security makes it a challenging concept to define, and thus requires an applied context (Brooks, 2010). CNI exacerbates this challenge as it introduces multiple sources of insecurity - security of supply, physical security, and cybersecurity to name a few (Pelizza, 2023). This paper will focus on the cyber-physical security, a system that is comprised of both physical elements and computational algorithms, of CNI (NIST, 2016).

Resilience

The definition of “resilience” faces comparable scrutiny and ambiguity. Generally, resilience refers to the capability of an entity following disruption. The disruption may take the form of a shock, disaster, fatigue, misfortune, or environmental change; and may take place over time or suddenly (Phillips & Chao, 2021; OED, 2023). Whilst the concept of resilience remains fairly constant, it subject to a broad spectrum of interpretations. In psychology, resilience is viewed as a personal trait concerning the “ability to cope with stress” (Olsson, et al., 2015). In material science, resilience can be applied to elasticity and resistence properties of a particular material. Policy documents consistently make reference to ‘bouncing back’ to a pre-disruption state or ‘bouncing forward’ to an alternative, and potentially, enhanced state. Thus, without a descriptive context, the ambiguity surrounding the word resilience makes it an unsuitable term for use in policy (Olsson, et al., 2015).

This gives rise to the first challenge with Scotland’s energy strategy. Scotland has fallen into the trap of unquestionally applying the polysemous word ‘resilience’. Without a contextual definition, ‘resilience’ becomes a buzzword, giving rise to “paradigm creep”: an unclear application resulting in broad and far-reaching interpretations (Tanner, et al., 2017). This obfuscates its meaning and utility and makes its measurement testing. Failure to distinguish between the resilience of functions and that of the structures established to achieve resilience gives rise to a lack of recognition for the broader societal implications in resilience thinking. After all, “one person’s resilience may be another person’s vulnerability” (Olsson, et al., 2015). By merely treating ‘resilience’ as a strategy for climate change, there is the potential for Scottish Government to overlook

the inherent political complexity and power dynamics of managing risk (Tanner, et al., 2017; Donoghue & Edmiston, 2020). Therefore, the absence of clarity suggests that Scotland's energy strategy is unlikely to enhance security of North Sea CNI.

The UN definition of resilience is "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management." (UNDRR, n.d.) This definition will be used going forward.

North Sea Critical Energy Infrastructure & Maritime Security

The North Sea energy sector kickstarted after the Second World War with the first substantial gas discovery in the Groningen area of The Netherlands (1959). Whilst this gave rise to speculation about natural gas reserves in the North Sea, debates around territorial ownership of the sea had already begun (Kemp, 2012). In 1958, the United Nations Convention on the Law of the Sea (UNCLOS) discussed the extension of North Sea coastal countries' rights to explore and exploit natural resources on their continental shelves[i] (United Nations, 1958). As defined by the Convention of the Continental Shelf: "the term "continental shelf" is used as referring (a) to the seabed and subsoil of the submarine areas adjacent to the coast but outside the area of the territorial sea, to a depth of 200 metres or, beyond that limit, to where the depth of the suprajacent waters admits of the exploitation of the natural resources of the said areas; (b) to the seabed and subsoil of similar submarine areas adjacent to the coasts of islands." (United Nations, 1958). The convention came into force in 1964 and the UK-based company, BP, made its first gas discovery in 1965 (BP, 2024). Since then, the energy sectors of Nordic countries and the UK have flourished to become a primary source of prosperity. With the transition to green technologies, the importance of the North Sea is amplified (Neal & Bueger, 2023).

The thriving energy sectors of these coastal countries have contributed to the dense network of critical maritime infrastructure in the North Sea. This comprises offshore

structures including oil and gas platforms, windfarms, and infrastructure facilitating the transmission of energy to land (e.g. underwater pipelines and electricity cables). These fixed structures are in addition to subsea communication cables that facilitate data flows and the internet (Bueger & Liebetrau, 2023). With future proposals for ‘energy islands’ and the rise of the Fourth Industrial Revolution (characterised by the fusion of physical, digital, and biological systems), the volume of critical maritime infrastructures will continue to grow (Schwab, K., 2017; DEA, n.d.). The strong interdependence between the physical structures and digital layers (for remote monitoring and control), generates significant challenges (Neal & Bueger, 2023). Typically, the challenges associated with maritime and terrestrial infrastructures are addressed by the same policy or strategy documents, and the governance of cyber-physical systems is characterised by separate cyber and physical policies or strategies. What is required is a policy encompassing all aspects of cyber and physical security for maritime infrastructures (and a similar policy for terrestrial infrastructures) (Bueger & Liebetrau, 2023). In turn, this will provide financial efficiencies arising from less duplication.

Maritime infrastructures are shrouded in legal complexity. The UNCLOS offers coastal countries full jurisdiction over territorial waters (within 12 nautical miles of its border), restricted authority over exclusive economic zones for exploitation and environmental protection and highly restricted authority over the high seas (Fig.2) (UN, 1958). However, many maritime infrastructures cross these jurisdictions (Bueger & Liebetrau, 2023). This gives rise to the question of responsibility.

[Figure 2]

The Nord Stream 2 subsea gas pipeline project serves as a prime example of this challenge. Proposed by Russia, Nord Stream 2 sought to establish an additional connection between Russia and Germany, traversing the Baltic Sea, thereby increasing Russia's capacity to gas export to Europe. Compared to its sister pipeline, Nord Stream, Nord Stream 2 faced a markedly different geopolitical climate, with a series of

constraints imposed by the Baltic States and other European member states (de Jong, 2023). For example, the Polish competition regulator expressed objections to the exclusive Russian ownership structure. Denmark hindered the project's progress by delaying the issuance of construction permits for transit through its territorial waters – one of five essential permits – citing concerns over environmental and shipping impacts. Simultaneously, the European Union implemented amendments to regulatory and compliance requirements for energy infrastructure. On 26 September 2022, an explosion damaged one of the lines of Nord Stream 2 and Nord Stream was rendered inoperable (de Jong, 2023). Swedish investigators suggest that, while identifying the responsible party is challenging, a state actor was likely involved (Ruiz and Sanger, 2024). The absence of policy on subsea infrastructure protection left responsibility for safeguarding the pipeline unclear, creating a regulatory gap that contributed to its vulnerability.

Operating across territories or connecting more than one country, maritime infrastructure security is thus dependent on strong international relationships. Whilst the North Sea countries have established collaborative clusters and projects, these positive relations do not imply responsibility for security nor adherence to UNCLOS. Central to this challenge is the “complex thicket of ownership” by “global business conglomerates” (Bueger & Liebetrau, 2021).

In addition to the vague stakeholder map, any notion of system boundaries is blurred in a cyber-physical system. This blurring of boundaries gives rise to a bigger attack surface for states, terrorists, or criminals to exploit. For example, modifications to the physical aspect of infrastructure are always observable. By observing these discernible changes, a skilful adversary could infer internal system settings and exploit the CNI (McMillin, et al., 2020). It is now apparent that preconceptions and concerns about Russian activity in the North Sea is well-founded. Cyber-physical systems need to be considered as a “whole” because, even if CNI is not the target, it may still be collateral damage in a cyber-attack elsewhere in the system. The NotPetya ransomware attack serves as a prime example. An attack targeted at Ukrainian IT infrastructure extensively and disproportionately disrupted major CNI, including container shipping corporation A.P.

Møller-Mærsk A/S (Greenberg, 2018). Application of discrete, unique policies or regulatory mechanisms to different parts of the CNI system introduces considerable barriers for effective cyber and physical security. This leaves the ‘backdoor open’ to global devastation (Choucri & Agarwal, 2019).

While there are notable exceptions, academic researchers, infrastructure security experts, and policymakers often overlook the potential threats, vulnerabilities, and status of critical maritime infrastructure. These can be attributed to critical infrastructure “invisibility” (Bueger & Liebetrau, 2021). CNI, like roads or bridges, have a tangible presence, are encountered daily and are debated publicly. However, as maritime infrastructures typically do not cause significant disruption during installation and are usually submerged, they are among the least conspicuous types of infrastructure. Seas and oceans are perceived as “empty voids” rather than hives of activity (Bueger & Liebetrau, 2021). The digital layer of CNI multiplies this ‘invisibility’ not least becuase connection can take place wirelessly (via Wi-Fi or satellite), and there is no tangible indication of ‘packet transfer’ in data flows. Data is divided into packets to facilitate transmission over a computer network (Yasar, 2022). Hence, it is to be expected, albeit unsurprising, that there is limited understanding among policymakers on how operations, regulations, responsibility and security measures of the network are inextricably linked.

With this mind, the University of Edinburgh and University of Copenhagen have established a partnership to ensure “that decarbonization strategies are not only understood in economic terms, but that the security implications are considered" (CeSeR, 2023). Therefore, in discussion with academia, Scotland’s green energy strategy plays a crucial role in shifting the CNI policy paradigm with regards to the security of North Sea CNI.

Scotland's Security Landscape

Scotland's security capability is subject to the rules of devolution – the transfer of UK powers to its national institutions.

Historically, the UK functioned within a 'Westminster Model' whereby all legislative power was held centrally. Before devolution, Scottish policy groups worked to lobby central government for solutions more appropriate for the Scottish people (Keating, 2010). Establishment of the Scottish Parliament offered the devolved administration autonomy to write separate policies on devolved matters, while the central UK government retained authority for state-wide policies – 'reserved matters' (MacKinnon, 2015). Of relevance to this discussion, reserved matters include defence (military forces) and national security; most aspects of energy (generation, transmission, distribution and supply of electricity, oil and gas; offshore installations and pipelines); foreign affairs (relations with territories outside the UK); and telecommunications (including internet services and electronic encryption) (*Scotland Act 1998)*. These reserved powers have inherently blurred boundaries, much like the jurisdictional and cyber-physical system boundaries of energy infrastructure.

As environmental and planning issues fall under devolved jurisdiction, Scotland holds authority to approve projects that drive infrastructure development. The Electricity Act 1989 extended this authority, empowering Scottish Ministers to determine the application of energy infrastructure. This includes the promotion of renewable energy, energy efficiency and onshore oil and gas licencing. Devolution also states that "any policy powers not explicitly reserved to the UK parliament are presumed to be devolved" (Webb & van der Horst, 2021). Hence, emergent policy domains can be left undefined, providing opportunity for the Scottish Government to shape inchoate energy policies. On one hand, Scotland cannot implement strategies subject to reserved powers, so policy publication merely serves as political rhetoric. On the other hand, cross-cutting and undeveloped legislation provides scope for Scotland to make its own decisions. Therefore, the security of its infrastructure ought to be prioritised, or at least, advocated when making planning decisions.

In evaluating policies and strategies published by the Scottish Government, there would appear to be a notable absence of consideration for the cyber or physical security of CNI.

The ‘Infrastructure Investment Plan 2021-22 to 2025-26’ correctly states that infrastructure “[produces] significantly more data creation, [and requires] common standards and cyber security”. However, the plan to address these trends is lacking (Scottish Government, 2021). The Energy Strategy states that “Energy security is a matter reserved to the UK Government. Scottish Ministers have responsibilities in responding to and managing civil contingencies, including large scale loss of electricity supply.” However, this document defines energy security as “having sufficient energy generation to meet the volume and type of energy demand at any point, and having the means to get that energy to the point of use” (Scottish Government, 2023).

Revisiting the challenges related to the definition of security, the Scottish Government refer to security in the context of supply and not cyber-physical. The Energy Strategy also states an ambition to achieve “a fully interconnected ‘North Sea Grid’ [to] ensure greater security and stability than what we would see with segregated systems.” This scales the attack surface, providing attackers with additional entry points and increasing vulnerability of the system. Based on these arguments, it can be concluded that the Green Energy Strategy will not inherently enhance the security of North Sea CNI.

Although the energy strategy may not explicitly address cyber-physical concerns, Scotland has published frameworks for cyber resilience and resilience of essential services (Scottish Government, 2020; 2021). Whilst these frameworks suggest recognition and intention to enhance cyber capability, they predominantly focus on preparing businesses for cyber threat, rather than prioritising the state’s own cyber defence. This may be attributable to the expectation of the role of the military (reserved power) in protecting maritime CNI and operations in the North Sea (HMG, 2022).

During the Cold War, Scotland held vital strategic importance in maintaining the transatlantic link between North America and Western Europe. It hosted a critical network of military and intelligence to support NATO forces in defending the northern flank and transatlantic communications lines (Depledge & Østhagen, 2021). When the Soviet Union disbanded, the threat to the northern flank diminished and some military and intelligence presence was withdrawn from Scotland, including the closure of several military bases (Royle, 2019). Among the remaining military bases, the Clyde Naval Base remains a vital element of UK Defence infrastructure, significantly contributing to local employment and bolstering the local economy (Wheeldon, 2022). Within the UK and NATO, Scotland's strategic importance diminished in the changing global context, “creating a ‘gap’ in the regional architecture of the High North” (Depledge & Østhagen, 2021). However, in recent years, Westminster has increasingly acknowledged that the UK has neglected defence of the North Atlantic and High North. To address this gap, the UK Government published ‘The UK’s Defence Contribution in the High North’, ‘National Strategy for Maritime Security’, and the ‘UK’s Arctic Policy Framework’ (MOD 2022, HMG 2022, FCDO 2023). Thus, highlighting that the capability of Scotland’s Green Energy Strategy to improve security of North Sea CNI is constrained by devolution and the level of support from Westminster (SNP, 2020).

At the time of writing, there are positive signs that the new administration in Whitehall is driving a more positive dialogue around how these boundaries can be administered better for common good (Parliament. House of Lords, 2024). The new National Protective Security Authority (NPSA), the UK’s National Technical Authority for physical and personnel protective security, and the National Cyber Security Centre (NCSC), the UK's National technical authority for cyber threats and Information Assurance, have also recently commenced regular dialogues with the devolved Administrations (Cabinet Office, 2023). The aim of such dialogues is to establish a more joined-up approach to make the UK less vulnerable and more resistant to national security threats.

Is Ireland Doing Any Better?

Scotland is not the only coastal nation battling with competing priorities of both the green energy transition and maritime security. Ireland encounters analogous challenges. However, it lacks the advantages afforded to Scotland as part of the UK, such as membership in a larger political union (on reserved matters) with a national security strategy and participation in NATO. Such benefits serve to address these issues more effectively.

Currently, Ireland's energy relies predominantly on subsea infrastructure, with approximately 75% of demand fulfilled via two subsea interconnectors originating from Scotland (McCabe & Flynn, 2023). Given the ongoing Russian and other terrorist threats, the Irish Government has committed to a more sovereign energy stance. Proposals include installing more windfarms in the Irish Sea and upgrading subsea energy connections between Ireland, the UK and Europe (Shortt, 2023; Government of Ireland, 2023). However, nearly four years after the initial public consultation, Ireland has yet to produce a National Security Strategy. The absence of such a document suggests a significant lack of real political will to in address these threats (O'Connor, 2023). In contrast, as part of its independence debate, Scotland has actively considered its national security policy position (Scottish Government, 2024).

Like the UK, Ireland relies on its military and coastguard capability to safeguard maritime infrastructure. This parallel vulnerability extends to the absence of necessary subsea capabilities and insufficiency of assets, within the Irish Naval Service, to fulfil maritime responsibilities effectively (Willett, 2011). Existing vessels are basic and lack NATO-standard equipment for successfully detecting subsea threats (McCabe & Flynn, 2023). Such substandard equipment is a consequence of Ireland's longstanding policy of military neutrality and consequent refusal to join NATO. Unsurprisingly, Ireland remains reliant on support from the British military, which is already overstretched (Gallagher, 2022). This continues the historic trend of inadequacy and reliance on outsourcing to other sovereignties.

One notable success of the Irish Government is its emphasis on CNI within its National Cyber Security Strategy (2019-2024). However, in spite of this focus on protecting CNI (as well as security of internet connectivity and data integrity) against targeted threats, there is no distinct reference to maritime infrastructure (Government of Ireland, 2019). Ireland has also followed the trend of using the polysemous word “resilience” without offering a clear definition in strategies. Consequently, it fails to enhance maritime CNI and mirrors the challenges faced by Scotland.

Conclusion

The growing threat to the energy sector from recent Russian and other terrorist activity has highlighted the strategic importance of maritime critical infrastructure, particularly in the North Sea. With Scotland’s sights set on being a net zero economy and trailblazer in renewable energy, even amid recent rollbacks on low-carbon commitments, greater attention must be given to the cyber-physical security of these interconnected maritime structures. Without such consideration, the remainder of the supply chain is left vulnerable to catastrophic damage. Despite Scotland’s best intentions to improve its cyber-physical security capabilities and strengthen international partnerships with Nordic countries, the Green Energy Strategy has yet to address shortfalls to improve North Sea CNI. This requires collaboration, trust and cooperation between the administrations in Westminster and those in Holyrood: a relationship that has historically been fraught as a consequence of differing political agendas. However, there have been encouraging indications that the new Labour government seeks to foster a more constructive dialogue between the devolved administrations.

This paper has attempted to articulate the challenges for Scotland regarding security of its maritime CNI, despite its role in energy – a vital social and economic conduit. Though maritime infrastructure may be out of sight, it should not be out of mind.

Governments should strive towards a universal definition of CNI, security and resilience. It is recommended that a more comprehensive international debate is facilitated to consolidate these definitions. CNI is considered essential for economic growth, societal

well-being, public protection, and the operation of key government duties, without which “catastrophic and far-reaching damage” could ensue (OECD, 2008). However, as sectors and infrastructure types differ globally, it is inherently difficult to comprehend without context. Security introduces further complexity owing to its multidimensional nature. This again emphasises the need for applied context. It would be advisable for governments to define their application of resilience within policies, since reliance on vague explanations hinders implementation. Scotland is not alone in its failure to provide clarity, resolution of which would provide direction as to where physical and financial resources are required.

Maritime CNI is surrounded by complicated legislation with blurred boundaries in ownership, responsibility, logistics, engineering design and implementation. It is subject to a ‘cloak of invisibility’, as subsea infrastructure is submerged and the digital layer is often intangible. This aspect is amplified in Scotland, where it is politically and geographically remote from and less accessible from the powerhouse of London. The cross-cutting nature of maritime CNI provides Scotland with an opportunity to champion innovation and progress in infrastructure security and contribute to greater cohesion across UK government departments (SNP, 2020). With the recent lapse of Scotland’s Critical Infrastructure Resilience framework, Scotland now has a window of opportunity to better define the term resilience and put forward a strategy for securing CNI in the North Sea and beyond.

References

Allison, G. (2022) *Russian spy ship off Scottish coast.* Available at: https://ukdefencejournal.org.uk/russian-spy-ship-off-scottish-coast/ (Accessed: 07 April 2024)

Asher, C. (2022) *What's the difference between wave energy and tidal energy?* Available at: https://www.sciencefocus.com/science/whats-the-difference-between-wave-energy-and-tidal-energy (Accessed: 06 April 2024)

Bolman, B. et al. (2018) *Oceans Report - Addressing SDG14 Issues with Factual Data and State of the Art Knowledge*. Available at: http://dx.doi.org/10.13140/RG.2.2.29210.59846

BP (2024) *Post-war – 1946-1970.* Available at: https://www.bp.com/en/global/corporate/who-we-are/our-history/post-war.html (Accessed: 08 April 2024)

Brooks, D. J. (2010) 'What is security: Definition through knowledge categorization', *Security Journal,* Volume 23, pp. 225-239. Available at: https://doi.org/10.1057/sj.2008.18

Brown, E. (1978) 'It's Scotland's oil?: Hypothetical boundaries in the North Sea — a case study', *Journal of Marine Policy,* 2(1), pp. 3-21. Available at: https://doi.org/10.1016/0308-597X(78)90056-8

Bueger, C. & Liebetrau, T. (2021) 'Protecting hidden infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy,* 42(3), pp. 391-413. Available at: https://doi.org/10.1080/13523260.2021.1907129

Bueger, C. & Liebetrau, T. (2023) 'Critical maritime infrastructure protection: What's the trouble?', *Marine Policy,* Volume 155. Available at: https://doi.org/10.1016/j.marpol.2023.105772

Cabinet Office (2023) *The UK Government Resilience Framework: 2023 Implementation Update*. Available at: https://assets.publishing.service.gov.uk/media/656def711104cf0013fa7498/The_UK_Government_Resilience_Framework_2023_Implementation_Update.pdf (Accessed: 08 September 2024)

Centre for Security Research (CeSeR) (2023) *New research funding for project on critical maritime infrastructure in the Greater North Sea region.* Available at: https://www.ceser.sps.ed.ac.uk/news-events/news/new-research-funding-project-critical-maritime-infrastructure-greater-north-sea (Accessed: 15 March 2024)

Choucri, N. & Agarwal, G. (2019) 'Securing the Long-Chain of Cyber-Physical Global Communication Infrastructure'*, IEEE International Symposium on Technologies for Homeland Security (HST*). Woburn, MA, USA, 5-6 Nov. Woburn: IEEE, pp. 1-7. Available at: https://doi.org/10.1109/HST47167.2019.9032933

Climate Change Committee (2024) *Progress in reducing emissions in Scotland 2023 Report to Parliament.* Available at: https://www.theccc.org.uk/wp-content/uploads/2024/03/Progress-in-reducing-emissions-in-Scotland-2023-Report-to-Parliament.pdf (Accessed: 21 September 2024)

Connolly, K. (2023) 'Russian spy network operating in North Sea, investigation claims', *The Guardian*, 19 April*.* Available at: https://www.theguardian.com/world/2023/apr/19/russian-spy-network-operating-in-north-sea-investigation-claims (Accessed: 07 April 2024)

Critical Infrastructure Protection Act of 2001. 42 U.S.C § 5195c (2001) Available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (Accessed: 05 April 2024)

Cunningham, R. (2019) *The Global Climate Emergency - Scotland's Response: Climate Change Secretary Roseanna Cunningham's statement.* Available at: https://www.gov.scot/publications/global-climate-emergency-scotlands-response-climate-change-secretary-roseanna-cunninghams-statement/ (Accessed: 05 April 2024)

Cybersecurity & Infrastructure Security Agency (CISA) (no date) *Critical Infrastructure Sectors.* Available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (Accessed: 05 April 2024)

Danish Energy Agency (DEA) (no date) *Denmark's Energy Islands.* Available at: https://ens.dk/en/our-responsibilities/offshore-wind-power/denmarks-energy-islands (Accessed: 08 April 2024)

de Jong, M. (2023) 'Tracing the downfall of the Nord Stream 2 gas pipeline', *WIREs Energy and Environement*, 13(1). Available at: https://doi.org/10.1002/wene.502

DeNardis, L. & Raymond, M. (2017) 'The Internet of Things as a Global Policy Frontier', *UC Davis Law Review,* 51(2). Available at: https://ssrn.com/abstract=3119909

Department of Defence (DoD) (2021) *Strategic Emergency Management Guideline 3 – Version 2 - Critical Infrastructure Resilience.* Available at: https://assets.gov.ie/90683/7d83eda8-4ff1-4a42-9c22-2d614c8a2d28.pdf (Accessed: 08 April 2024)

Depledge, D. & Østhagen, A. (2021) 'Scotland: A Touchstone for Security in the High North?', *The RUSI Journal,* 166(6-7), pp. 46-62. Available at: https://doi.org/10.1080/03071847.2022.2036229

Donoghue, M. & Edmiston, D. (2020) 'Gritty citizens? Exploring the logic and limits of resilience in UK social policy during times of socio-material insecurity', *Critical Social Policy,* 40(1), pp. 7-29. Available at: https://doi.org/10.1177/0261018319825547

Earle, S. (2021) 'Wave and Tidal Energy', in *Environmental Geology.* Available at: https://environmental-geol.pressbooks.tru.ca/front-matter/introduction/ (Accessed: 04 April 2024)

Edmond, C. (2020) *A new tidal energy project just hit a major milestone in Scotland.* Available at: https://www.weforum.org/agenda/2020/01/tidal-renewable-energy-turbine-electricity-generation-scotland/ (Accessed: 06 April 2024)

Foreign, Commonwealth & Development Office (FCDO) (2023) *Looking North: the UK and the Arctic.* Available at: https://assets.publishing.service.gov.uk/media/63e38ed3e90e0762637e30d0/looking-north-the-uk-and-the-arctic-the-uks-arctic-policy-framework.pdf (Accessed: 11 April 2024)

Gallagher, C. (2022) 'British surveillance ship to monitor subsea cables in Irish economic zone' *The Irish Times*, 28 July. Available at: https://www.irishtimes.com/ireland/2022/07/28/british-surveillance-ship-will-monitor-subsea-cables-in-irish-economic-zone/ (Accessed: 11 April 2024)

Google (2024) *Books Ngram Viewer.* Available at: https://books.google.com/ngrams/ (Accessed: 27 March 2024)

Government of Ireland (2019) *National Cyber Security Strategy.* Available at: https://www.gov.ie/en/publication/8994a-national-cyber-security-strategy/ (Accessed: 11 April 2024)

Government of Ireland (2023) *Accelerating Ireland's Offshore Energy Programme Policy Statement on the Framework for Phase Two Offshore Wind.* Available at: https://www.gov.ie/pdf/?file=https://assets.gov.ie/249823/bbd8b13c-73cd-46d4-9902-533fbf03d7fe.pdf#page=null (Accessed: 11 April 2024)

Gray, N. (2023) *Update on Scotland's renewables and wind power potential.* Available at: https://www.gov.scot/publications/renewables-and-wind-power-update-to-scottish-affairs-committee/ (Accessed: 06 April 2024)

Greenberg, A. (2018) *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Accessed: 09 April 2024)

HM Government (HMG) (2019) *Devolution: Factsheet.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/770709/DevolutionFactsheet.pdf (Accessed: 10 April 2024)

HM Government (HMG) (2022) *National Strategy for Maritime Security* (CP 724). Available at: https://assets.publishing.service.gov.uk/media/630880c5e90e0729d9ab15fc/national-strategy-for-maritime-security-web-version.pdf (Accessed: 11 April 2024)

HM Treasury (2010) *National Infrastructure Plan 2010.* Available at: https://assets.publishing.service.gov.uk/media/5a74a5cf40f0b619c86594cb/nip_2010.pdf (Accessed: 04 March 2024)

Ismay, L. (2001) *NATO common infrastructure.* Available at: https://www.nato.int/archives/1st5years/chapters/10.htm (Accessed: 04 April 2024)

Joint Committee on the National Security Strategy (JCNSS) (2022) Critical national infrastructure and climate adaptation. Available at: https://committees.parliament.uk/work/1659/critical-national-infrastructure-and-climate-adaptation/ (Accessed: 08 April 2024)

Keating, M. (2010) *The Government of Scotland: Public Policy Making after Devolution.* 2nd ed. Edinburgh: Edinburgh Univeristy Press.

Kemp, A. (2012) *The Official History of North Sea Oil and Gas Volume 1: The Growing Dominance of the State.* London: Routledge. Available at: https://doi.org/10.4324/9780203806241

Kerr, S. (2024) 'Scotland ditches 2030 climate target as being 'out of reach'', *Financial Times*, 18 April. Available at: https://www.ft.com/content/6960a200-2ccd-4279-ad1f-5ad1e749310d (Accessed: 20 September 2024)

MacKinnon, D. (2015) 'Devolution, state restructuring and policy divergence in the UK', *The Geographical Journal,* 181(1), pp. 47-56. Available at: https://doi.org/10.1111/geoj.12057

McCabe, R. & Flynn, B. (2023) 'Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure, *European Security.* Available at: https://doi.org/10.1080/09662839.2023.2248001

McMillin, B. et al. (2020) 'Security in the Cyber-Physical Electric Power Infrastructure, in S. Roy & S. K. Das (eds) *Principles of Cyber-Physical Systems An Interdisciplinary Approach.* Cambridge: Cambridge University Press, pp. 252-292. Available at: https://doi.org/10.1017/9781107588981.014

McNamara, E. M. (2024) Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure. Available at: https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/ (Accessed: 02 September 2024)

Ministry of Defence (MOD) (2022) *The UK's Defence Contribution in the High North.* [Online] Available at: https://www.gov.uk/government/publications/the-uks-defence-contribution-in-the-high-north (Accessed: 11 April 2024)

National Coordinator for Security and Counterterrorism (NCTV) (2018) *Resilient critical infrastructure.* Available at: https://english.nctv.nl/topics/critical-infrastructure-protection/documents (Accessed: 05 April 2024)

National Coordinator for Security and Counterterrorism (NCTV) (no date) *Critical Infrastructure (protection).* Available at: https://english.nctv.nl/topics/critical-infrastructure-protection (Accessed: 05 April 2024)

National Infrastructure Security Co-ordination Centre (NISCC) (2004) *Good Practice Guide To Telecommunications Resilience.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/85910/flu_niscc.pdf (Accessed: 04 April 2024)

National Institute of Standards and Technology (NIST) (2016) *Cyber Physical Systems.* Available at: https://www.nist.gov/itl/ssd/cyber-physical-systems (Accessed: 08 April 2024)

National Protective Security Authority (NPSA) (2023) *Critical National Infrastructure.* Available at: https://www.npsa.gov.uk/critical-national-infrastructure-0 (Accessed: 05 April 2024)

North Atlantic Treaty Organization (NATO) (2024) *NATO hold first meeting of Critical Undersea Infrastructure Network*. Available at: https://www.nato.int/cps/en/natohq/news_225582.htm (Accessed: 02 September 2024)

North Atlantic Treaty Organization (NATO) (2022) *Relations with Ireland*. Available at: https://www.nato.int/cps/en/natohq/topics_51979.htm (Accessed: 27 September 2024)

Neal, A. & Bueger, C. (2023) *NATO and the North Sea: Securing the Green Energy Transition.* Available at: https://www.rusi.org/explore-our-research/publications/commentary/nato-and-north-sea-securing-green-energy-transition (Accessed: 27 March 2024)

New Zealand Lifelines Council (NZLC) (2023) *Aotearoa New Zealand's Critical Infrastructure - A National Vulnerability Assessment - Part B: Infrastructure Resilience in New Zealand.* Available at: https://www.civildefence.govt.nz/assets/Uploads/documents/lifelines/NVA-Part-B-Main-report-v1.0-Sept-2023.pdf (Accessed: 05 April 2024)

New Zealand Lifelines Council (NZLC) (2023) *Aotearoa New Zealand's Critical Infrastructure - A National Vulnerability Assessment - Part C: Infrastructure Sectors and Hazards Assessment.* Available at: https://www.civildefence.govt.nz/assets/Uploads/documents/lifelines/NVA-Part-C-Sectors-and-Hazards-v1.0-Sept-2023.pdf (Accessed: 05 April 2024)

Newnham, R. (2011) 'Oil, Carrots, and Sticks: Russia's Energy Resources as a Foreign Policy Tool', *Journal of Eurasian Studies,* 2(2), pp. 134-143. Available at: https://doi.org/10.1016/j.euras.2011.03.004

North Sea Energy Atlas (no date) *Project Atlas North Sea Energy Map,* Project Atlas. Available at: https://northseaenergy.projectatlas.app/atlas/make-your-own-map/visibility

O'Connor, (2023) 'Missing in action: Ireland's national security strategy has been in the works since 2019', *The Journal*, 12 Aug. Available at: https://www.thejournal.ie/no-national-security-strategy-taoiseach-department-6138880-Aug2023/ (Accessed: 27 September 2024)

Olsson, L. et al. (2015) 'Why resilience is unappealing to social science: Theoretical and empirical investigations of the scientific use of resilience', *Science Advances,* 1(4). Available at: https://doi.org/10.1126/sciadv.1400217

Organisation for Economic Co-operation and Development (OECD) (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security.* Available at: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf (Accessed: 27 March 2024)

Osgood, R. E. (1954) 'Ideals and Self-Interest in America's Foreign Relations: the Great Transformation of the Twentieth Century', *International Affairs,* 30(2), pp. 264-265. Available at: https://doi.org/10.2307/2607636

Oxford English Dictionary (2023) 'Resilience, N.' Oxford: Oxford University Press. Available at: https://www.oed.com/dictionary/resilience_n?tl=true (Accessed: 28 March 2024)

Parliament. House of Lords (2024) *King's Speech 2024: Devolved affairs*. London: The Stationary Office. Available at: https://researchbriefings.files.parliament.uk/documents/LLN-2024-0031/LLN-2024-0031.pdf (Accessed: 08 September 2024)

Pelizza, A. (2023) 'Securitizing the infrastructural Europe, infrastructuring a securitized Europe', in N. Klimburg-Witjes and P. Trauttmansdroff (ed) *Technopolitics and the Making of Europe.* Oxon, UK: Routledge, pp. 162-164. Available at: https://doi.org/10.4324/9781003267409

Phillips, F. Y. & Chao, A. (2021) 'Rethinking Resilience: Definition, Context, and Measure', *IEEE Transactions of Engineering Management,* pp. 1-8. Available at: https://doi.org/10.1109/TEM.2021.3139051

Rees, J. & Rees, C. J. (2023) 'Cyber-Security and the Changing Landscape in Critical National Infrastructure: State and Non-state Cyber-Attacks on Organisations, Systems and Services', in R. Montasari (ed) *Applications for Artificial Intelligence and Digital Forensics in National Security.* Switzerland: Springer Cham, pp. 67-89. Available at: https://doi.org/10.1007/978-3-031-40118-3_5

Rothschild, E. (1995) 'What Is Security?', *Daedalus,* 124(3), pp. 53-98. Available at: http://www.jstor.org/stable/20027310

Royle, T. (2019) *Facing the Bear: Scotland and the Cold War.* Edinburgh: Birlinn.

Ruiz, R. & Sanger, D. (2024) 'Sweden Closes Investigation of Pipeline Blasts, but Stays Silent on Cause', *The New York Times*, 7 Feb. Available at: https://www.nytimes.com/2024/02/07/world/europe/sweden-nord-stream-pipeline.html (Accessed: 27 September 2024)

Schwab, K. (2019) *The Fourth Industrial Revolution.* New York: Penguin Random House.

Scotland Act 1998, c. 46. Available at: https://www.legislation.gov.uk/ukpga/1998/46/schedule/5 (Accessed: 08 April 2024)

Scottish Enterprise (no date) *Join Scotland's energy transition manufacturing supply chain.* Available at: https://www.scottish-enterprise.com/support-for-businesses/innovation-digital-and-data/scotlands-energy-transition-opportunity/manufacturing-for-the-energy-transition-supply-chain (Accessed: 02 September 2024)

Scottish National Party (SNP) (2020) *SNP Submission to the Integrated Review.* Available at: https://www.stewartmcdonald.scot/files/snp-submission-to-the-integrated-review-november-2020.pdf (Accessed: 11 April 2024)

Shortt, R. (2023) *Four successful bidders in first offshore wind auction.* Available at: https://www.rte.ie/news/business/2023/0511/1382911-offshore-windfarm-electricity-auction/ (Accessed: 11 April 2024)

Steola, R., Luiijf, E. & Theocharidou, M. (2016) 'Critical Infrastructures, Protection and Resilience', in R. Setola, V. Rosato, E. Kyriakides, E. Rome (eds) *Managing the Complexity of Critical Infrastructures.* Switzerland: Springer Cham, pp. 1-18. Available at: https://doi.org/10.1007/978-3-319-51043-9_1

Tanner, T., Bahadur, A. & Moench, M. (2017) *Challenges for resilience policy and practice,* ODI Global Advisory. Available at: http://dx.doi.org/10.13140/RG.2.2.30130.30402

The European Marine Energy Centre (EMEC) Ltd (2024) *About Us.* Available at: https://www.emec.org.uk/about-us/ (Accessed: 07 April 2024)

The Scottish Government (2020) *Update to the Climate Change Plan 2018 - 2032.* [Online] Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2020/12/securing-green-recovery-path-net-zero-update-climate-change-plan-20182032/documents/update-climate-change-plan-2018-2032-securing-green-recovery-path-net-zero/update-climate-change-plan-2018-2032-securing-green-recovery-path-net-zero/govscot%3Adocument/update-climate-change-plan-2018-2032-securing-green-recovery-path-net-zero.pdf (Accessed: 27 March 2024)

The Scottish Government (2017) *Nordic Baltic policy statement.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/speech-statement/2017/09/points-north-scottish-governments-nordic-baltic-policy-statement/documents/00525147-pdf/00525147-pdf/govscot%3Adocument/00525147.pdf (Accessed: 07 April 2024)

The Scottish Government (2020) *Keeping Scotland Running Resilient Essential Services Scottish Government's Strategic Framework 2020-2023.* Available at: https://ready.scot/sites/default/files/2022-12/keeping-scotland-running-2020-final-UpdateDecember2022.pdf (Accessed: 10 April 2024)

The Scottish Government (2021) *Infrastructure Investment Plan for Scotland 2021-22 to 2025-26.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2021/02/national-mission-local-impact-infrastructure-investment-plan-scotland-2021-22-2025-26/documents/national-mission-local-impact-infrastructure-investment-plan-scotland-2021-22-2025-26/national-mission-local-impact-infrastructure-investment-plan-scotland-2021-22-2025-26/govscot%3Adocument/national-mission-local-impact-infrastructure-investment-plan-scotland-2021-22-2025-26.pdf (Accessed: 27 March 2024)

The Scottish Government (2021) *Scottish Government and Scottish Green Party Draft Shared Policy Programme.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/agreement/2021/08/scottish-government-and-scottish-green-party-shared-policy-programme/documents/scottish-government-and-scottish-green-party-draft-shared-policy-programme/scottish-government-and-scottish-green-party-draft-shared-policy-programme/govscot%3Adocument/SG%2BSGP%2BTalks%2B-%2BDraft%2BPolicy%2BProgramme%2B-%2Bversion%2B7%2B-%2BFINAL%2B-%2BOFFSEN.pdf (Accessed: 07 April 2024)

The Scottish Government (2021) *The Strategic Framework for a Cyber Resilient Scotland.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2021/02/strategic-framework-cyber-resilient-scotland/documents/strategic-framework-cyber-resilient-scotland/strategic-framework-cyber-resilient-scotland/govscot%3Adocument/ (Accessed: 10 April 2024)

The Scottish Government (2022) *Strengthening Scotland's Nordic ties.* Available at: https://www.gov.scot/news/strengthening-scotlands-nordic-ties/ (Accessed: 08 April 2024)

The Scottish Government (2022) *Written evidence submitted by the Scottish Government.* (NIC0018). Available at: https://committees.parliament.uk/writtenevidence/43795/pdf/ (Accessed: 20 March 2024)

The Scottish Government (2023) *Draft Energy Strategy and Just Transition Plan.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2023/01/draft-energy-strategy-transition-plan/documents/draft-energy-strategy-transition-plan/draft-energy-strategy-transition-plan/govscot%3Adocument/draft-energy-strategy (Accessed: 06 April 2024)

The Scottish Government (2024) *An independent Scotland's place in the world.* Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/research-and-analysis/2024/03/building-new-scotland-independent-scotlands-place-world/documents/independent-scotlands-place-world/independent-scotlands-place-world/govscot%3Adocument/independent-scotlands-place-world.pdf (Accessed: 27 September 2024)

Tyrrell, P. J. (2001) 'Protecting the National Critical Infrastructure: The Human Dimension From a Government Perspective', *Journal of Information Warfare,* 1(2), pp. 76-86. Available at: https://www.jstor.org/stable/26486097

United Nations Office for Disaster Risk Reduction (UNDRR) (no date) *Resilience.* Available at: https://www.undrr.org/terminology/resilience (Accessed: 02 April 2024)

United Nations (UN) (1958) *Convention on the Continental Shelf.* Available at: https://legal.un.org/ilc/texts/instruments/english/conventions/8_1_1958_continental_shelf.pdf (Accessed: 08 April 2024)

Webb, J. & van der Horst, D. (2021) 'Understanding policy divergence after United Kingdom devolution: Strategic action fields in Scottish energy efficiency policy', *Energy Research & Social Science,* Volume 78. Available at: https://doi.org/10.1016/j.erss.2021.102121

Wheeldon, H. (2022) *Vital Importance of HMNB Clyde (Updated) By Howard Wheeldon, FRAeS, Wheeldon Strategic Advisory Ltd.* Available at: https://battle-updates.com/vital-importance-of-hmnb-clyde-updated-by-howard-wheeldon-fraes-wheeldon-strategic-advisory-ltd/ (Accessed: 09 September 2024)

Willett, L. (2011) *Mind the Gap: Strategic Risk in the UK's Anti-Submarine Warfare Capability.* Available at: https://www.rusi.org/explore-our-research/publications/commentary/mind-gap-strategic-risk-uks-anti-submarine-warfare-capability (Accessed: 11 April 2024)

World Wide Fund for Nature (WWF) (2021) *Scotland's Climate Story: An Overview.* Available at: https://www.wwf.org.uk/sites/default/files/2021-10/SCOTLANDS%20CLIMATE%20STORY%20OVERVIEW_0.pdf (Accessed: 05 April 2024)

Yasar, K. (2022) *What is a network packet and how does it work?* Available at: https://www.techtarget.com/searchnetworking/definition/packet (Accessed: 09 April 2024)

Tables and Figures

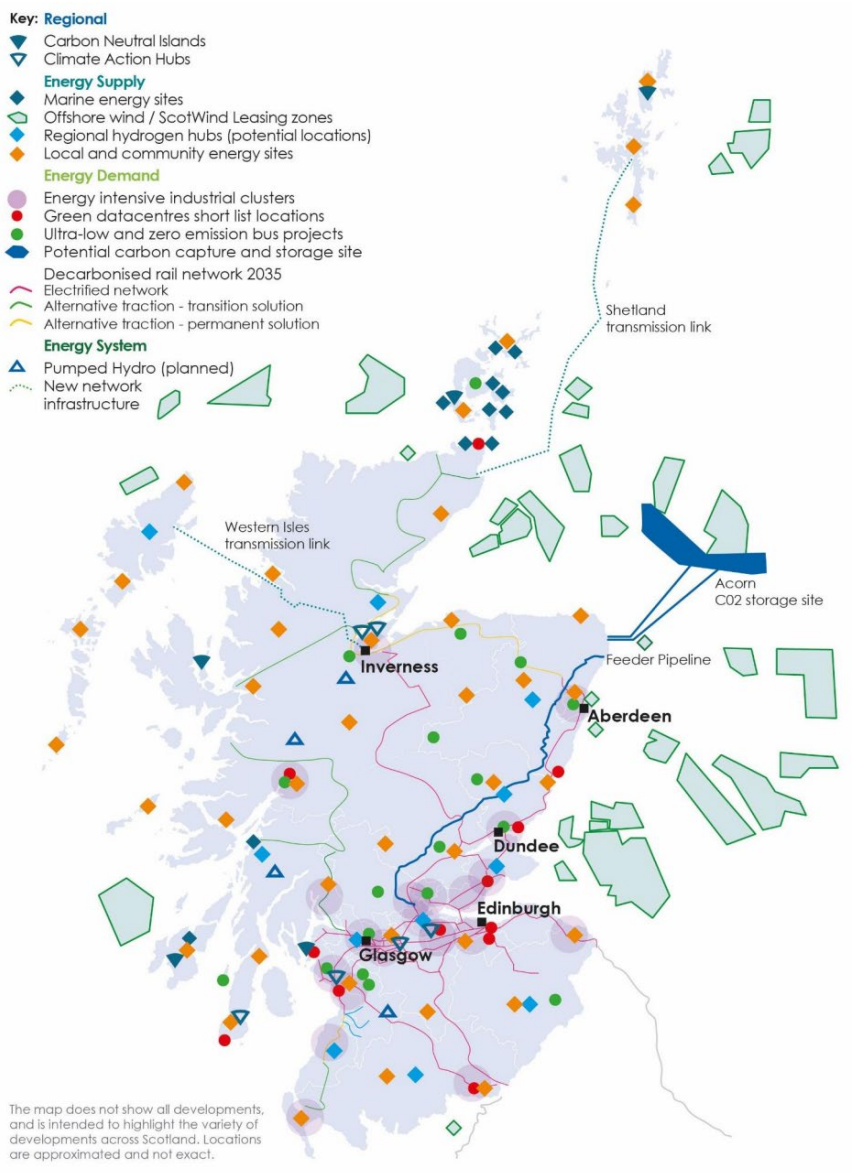

Figure 1: Regional and National Energy Opportunities (Scottish Government, 2023)

Table 1: National Definitions of Critical National Infrastructure

Country	Critical National Infrastructure Definition
United States	“systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” (42 U.S.C. 5195c (e)) (Congress, 2001)
United Kingdom	“Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state.” (NPSA, 2023)
Ireland	“Critical National Infrastructure can be defined as being of unique national importance, which if disrupted or destroyed would have significant national level effects and may impact across a number of sectors.” (DoD, 2021)
New Zealand	“Essential and enabling assets, systems, services and supply chains. Principles • Essential for the economy, national security, public safety and the continuous provision of basic public and other infrastructure services; and/or • Disruption would severely prejudice the functioning or stability of the nation or national security. Criteria • Of significant economic, public, social and strategic importance; and/or • Service disruption could affect the nation’s ability to function, deliver basic public services, or maintain law and order; and/or • Infrastructure failure could have a significant effect on the environment, the health or safety of the public or the functioning of other critical infrastructure.” (NZLC, 2023)
Netherlands	"Critical processes are processes that could result in severe social disruption in the event of their failure or disruption." (NCTV, 2018)

Table 2: Critical National Infrastructure Sectors in Selected Countries

Sector	US	UK	Ireland	New Zealand	Netherlands
Chemicals	X	X	X		X
Communications	X	X		X	X
Defence	X	X			X
Energy (incl. Nuclear)	X	X	X	X	X
Finance	X	X	X	X	X
Food	X	X	X		
Government	X	X	X		X
Healthcare	X	X	X		X
ICT	X	X	X	X	X
Manufacturing	X		X		
Safety	Emergency Services	Emergency Services	National Security, Policing & Public Safety Infrastructure		Public Order & Safety
Transport	X	X	X	X	X
Water	X	X		X	X
Waste	X		X	X	
Other Sectors	Commercial Facilities, Dams	Space	Logistical Supply Chains	Flood Protection	

(**Sources:** US - CISA, n.d., UK - NPSA, 2023, Ireland - Department of Defence, 2021, New Zealand - NZLC, 2023, Netherlands - NCTV, 2018)

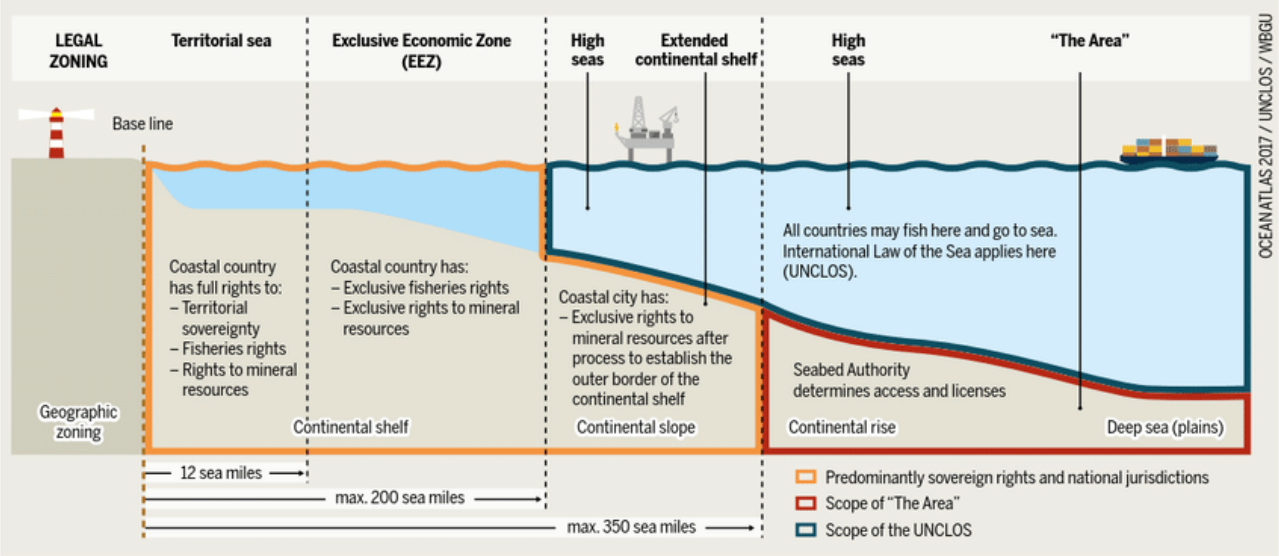

Figure 2: Legal Boundaries of the Ocean (Bolman, et al., 2018)