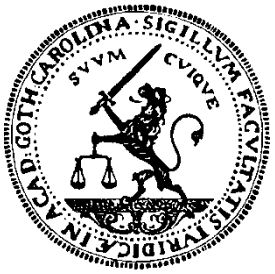


FACULTY OF LAW

LUND UNIVERSITY

Isabelle Jellhede

Governing Critical Subsea Infrastructure in the Baltic Sea:

Complementing UNCLOS Through the EU Resilience Framework

JURM02 Graduate thesis

Graduate thesis, Master of Laws program

30 higher education credits

Supervisor: Olena Bokareva

Semester: Spring 2026

Table of contents

Summary

This thesis examines the extent to which the European Union's resilience framework, particularly the Critical Entities Resilience Directive (CER) and the Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2), complements the legal framework established under the United Nations Convention on the Law of the Sea (UNCLOS) regarding the governance and protection of critical subsea infrastructure in the Baltic Sea. The thesis focuses specifically on submarine cables and pipelines and addresses the structural limitations of existing legal frameworks in relation to contemporary threats.

The thesis applies a legal dogmatic method and analyses relevant sources of public international law and EU law through treaty interpretation and EU legal methodology. UNCLOS is interpreted in accordance with the Vienna Convention on the Law of Treaties (VCLT), while the analysis of EU law proceeds in light of the teleological and systematic interpretative methods commonly applied within EU law.

The thesis demonstrates that UNCLOS establishes the foundational legal framework governing submarine cables and pipelines through its allocation of rights and jurisdiction between States in different maritime zones. While coastal States possess comparatively broad enforcement powers within the territorial sea, the Convention relies more heavily on flag State jurisdiction, due regard obligations and inter-State cooperation beyond territorial waters. The thesis argues that this structure creates practical and legal challenges regarding the protection of subsea infrastructure against contemporary threats in the Baltic Sea, particularly where incidents involve foreign-flagged vessels, multiple jurisdictions or suspected hybrid threats.

In contrast to UNCLOS, the CER and NIS2 Directives establish a broader resilience-oriented framework focused more directly on the protection, continuity and risk management of critical infrastructure and essential services. Through obligations relating to risk assessments, cybersecurity, supervision and cross-border cooperation, the Directives seek to reduce vulnerabilities and strengthen the management of disruptions affecting subsea infrastructure.

The thesis argues that the EU resilience framework complements the UNCLOS regime by addressing several challenges that UNCLOS was not originally designed to manage. At the same time, the thesis emphasises that the EU framework continues to operate within the broader jurisdictional structure established under UNCLOS and therefore cannot fully eliminate the Convention's structural limitations. Nevertheless, the relationship between UNCLOS and the EU resilience framework is particularly significant in the

Baltic Sea context due to the high degree of regional integration between the surrounding coastal States and the transnational nature of subsea infrastructure in the region.

Sammanfattning

Denna uppsats undersöker i vilken utsträckning EU:s resiliensramverk, särskilt CER-direktivet (Critical Entities Resilience Directive) och NIS2-direktivet (Directive on Measures for a High Common Level of Cybersecurity across the Union), kompletterar det rättsliga ramverk som etableras genom Förenta nationernas havsrättskonvention (UNCLOS) avseende styrningen och skyddet av kritisk undervattensinfrastruktur i Östersjön. Uppsatsen fokuserar särskilt på undervattenskablar och rörledningar samt de strukturella utmaningar som samtida hot medför för befintliga rättsliga ramverk.

Uppsatsen tillämpar en rättsdogmatisk metod och analyserar relevanta rättskällor inom folkrätt och EU-rätt genom traktattolkning och EU-rättslig metod. UNCLOS tolkas i enlighet med Wienkonventionen om traktaträtten (VCLT), medan analysen av EU-rätten genomförs mot bakgrund av de teleologiska och systematiska tolkningsmetoder som vanligtvis tillämpas inom EU-rätten.

Uppsatsen visar att UNCLOS etablerar det grundläggande rättsliga ramverket för undervattenskablar och rörledningar genom sin reglering av rättigheter och jurisdiktion mellan stater i olika maritima zoner. Medan kuststater har relativt långtgående tillsyns- och verkställighetsbefogenheter inom territorialhavet, bygger konventionen i högre grad på flaggstatsjurisdiktion, *due regard*-skyldigheter och mellanstatligt samarbete utanför territorialhavet. Uppsatsen argumenterar för att denna struktur skapar praktiska och rättsliga utmaningar i relation till skyddet av undervattensinfrastruktur mot samtida hot i Östersjön, särskilt när incidenter involverar utlandsflaggade fartyg, flera jurisdiktioner eller misstänkta hybridhot.

Till skillnad från UNCLOS etablerar CER- och NIS2-direktiven ett bredare resiliensinriktat ramverk som mer direkt fokuserar på skydd, kontinuitet och riskhantering av kritisk infrastruktur och samhällsviktiga tjänster. Genom skyldigheter avseende riskbedömningar, cybersäkerhet, tillsyn och gränsöverskridande samarbete syftar direktiven till att minska sårbarheter och stärka hanteringen av störningar som påverkar undervattensinfrastruktur.

Uppsatsen argumenterar för att EU:s resiliensramverk kompletterar UNCLOS-regimen genom att adressera flera styrnings- och samordningsrelaterade utmaningar som UNCLOS ursprungligen inte utformades för att hantera. Samtidigt betonas att EU:s ramverk fortsatt verkar inom den bredare jurisdiktionsstruktur som etableras genom UNCLOS och därför inte fullt ut kan eliminera konventionens strukturella begränsningar. Relationen mellan UNCLOS och EU:s resiliensramverk är emellertid särskilt betydelsefull i Östersjökontexten på grund av den höga graden av regional integration mellan de omkringliggande kuststaterna och undervattensinfrastrukturens gränsöverskridande karaktär i regionen.

Preface

Jag vill inledningsvis rikta ett stort tack till min handledare Olena Bokareva för ditt stöd, din konstruktiva återkoppling och värdefulla vägledning genom hela uppsatsprocessen. Särskilt vill jag tacka dig för att ha väckt mitt intresse för havsrätten och för de spännande möjligheter som du har erbjudit längs vägen.

Jag vill även rikta ett varmt tack till min familj för allt stöd, all uppmuntran och den tilltro ni alltid har visat mig. Vidare vill tacka mina fina vänner för att ha gjort studietiden till så mycket mer än bara studier och för all glädje ni har skänkt mig längs vägen.

Slutligen vill jag tacka Lund för åren som har format mig, för alla människor jag har fått möta och för alla de stunder som gjort min studietid så speciell.

Isabelle Jellhede,
Lund, maj 2026

Abbreviations

CER	Critical Entities Resilience Directive
CJEU	Court of Justice of the European Union
EEZ	Exclusive Economic Zone
ENISA	European Union Agency for Cybersecurity
EU	European Union
HELCOM	Helsinki Commission
ICJ	International Court of Justice
IMO	International Maritime Organization
MARPOL	International Convention for the Prevention of Pollution from Ships, as modified by the 1978 Protocol
NIS2	Directive on Measures for a High Common Level of Cybersecurity Across the Union
ILA	International Law Association
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
VCLT	Vienna Convention on the Law of Treaties

1 Introduction

1.1 Background

Although submarine cables have formed a part of global communication systems since the 1800s, critical maritime infrastructure has in recent years received unprecedented political and legal attention, particularly following the series of disrupting incidents affecting infrastructure in the Baltic Sea.[1] Prior to 2022, disruptions to such infrastructure were generally treated as isolated accidents or technical failures. The explosions affecting the Nord Stream pipelines in September 2022, however, marked a significant turning point, as it exposed the vulnerability of critical subsea infrastructure and highlighted their need for enhanced protection, particularly against intentional damage.[2]

The incident transformed maritime infrastructure such as submarine cables and pipelines, which had previously been overlooked, into a political top priority and a matter of strategic importance. It triggered increased policy activity and the development of new strategies and regulatory initiatives aimed at strengthening the protection and resilience of maritime infrastructure, with NATO and the European Union being especially active in this regard.[3] Subsequent incidents involving cables and pipelines in the Baltic Sea have further intensified concerns relating to the resilience, governance and protection of such critical infrastructure.[4] The vulnerability of the infrastructure is further said to increase as the amount of maritime installations grow.[5] In response to the increasing number of disruptions, efforts to strengthen regional cooperation and surveillance have intensified. In May 2025, Sweden, together with other Baltic Sea States, the European Union, Norway and Iceland, signed a Memorandum of Understanding concerning enhanced protection of critical undersea infrastructure.[6] Following the

[1] European Commission, Joint Research Centre, 'Subsea cables: how vulnerable are they and can we protect them?' (8 August 2025) https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en accessed 3 May 2026.

[2] Daniel Hernandez-Benito, 'Damages to Submarine Cables and Pipelines in Times of Peace and War: The Nord Stream Sabotage', (2024), 16(1) *Amsterdam Law Forum* 1, 1; Yula Koshino, 'The changing submarine cables landscape: Expanding the EU's role in the Indo-Pacific' (European Union Institute for Security Studies, Brief, 30 October 2024) https://www.iss.europa.eu/publications/briefs/changing-submarine-cables-landscape accessed 2 March 2026.

[3] Christian Bueger and Tobias Liebetrau, 'Critical Maritime Infrastructure Protection: What's the Trouble?' (2023) 155 *Marine Policy* 105772, 1.

[4] Hernandez-Benito (n 2), 1.

[5] Marcos Julien Alexopoulos, Arto Niemi, Bartosz Skobiej and Frank Sill Torres, 'Examination of the Critical Infrastructure Resilience Directive from the Maritime Point of View' (2025) 63(2) Journal of Common Market Studies 667, 667.

[6] Swedish Ministry of Defence and Ministry for Foreign Affairs 'Sweden signs Memorandum of Understanding on the protection of critical undersea infrastructure' (21 May

Estlink 2 incident in late 2024, NATO also launched the "Baltic Sentry" mission aimed at strengthening surveillance, situational awareness and deterrence in the Baltic Sea region.[7]

Submarine cables have long been of strategic importance, both for global communications and intelligence activities. Already during the Cold War, underwater cables were targeted in espionage operations, illustrating their longstanding geopolitical significance. Although confirmed State-sponsored attacks against subsea infrastructure were for a long time considered unlikely, scholars nevertheless warned that such infrastructure could become a target in future conflicts.[8] Recent incidents in the Baltic Sea suggest that these concerns are no longer merely hypothetical.

Modern societies are structurally dependent on subsea infrastructure for digital communication, energy transmission, financial systems, trade and broader societal functioning. Underwater cables carry 99 % of intercontinental internet traffic, while pipelines and electricity cables play a central role in energy security and cross-border connectivity.[9] As a result, disruptions affecting such infrastructure may have far-reaching societal, economic and geopolitical consequences extending well beyond the immediately affected region. The broader implications of disruptions affecting maritime infrastructure have also become increasingly visible in recent geopolitical crises. While writing this thesis, disruptions affecting the Strait of Hormuz have demonstrated how disturbances in strategically important maritime regions can generate cascading effects across interconnected sectors, including global trade, energy markets and food supply chains.[10] Similarly to the disruptions in the Baltic Sea, the events in the Hormuz Strait underscore the extent to which modern societies depend on secure and resilient maritime infrastructure.

Due to the inherent transnational nature of submarine cables and their tendency to operate across several maritime zones, the protection of them can

---

2025) https://www.government.se/press-releases/2025/05/sweden-signs-memorandum-of-understanding-on-the-protection-of-critical-undersea-infrastructure/ Accessed 3 May 2026.

[7] North Atlantic Treaty Organization 'NATO launches "Baltic Sentry" to increase critical infrastructure security' (14 January 2025) https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security accessed 4 May 2026.

[8] Wolff Heintschel von Heinegg, 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection Submarine Communication Cables under International Law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE Publications 2013) 293, 295.

[9] European Commission, Joint Research Centre (n 1).

[10] UN Trade and Development, *Strait of Hormuz Disruptions: Implications for Global Trade and Development (*10 March 2026) 2 and 17; BBC News, 'Why the Strait of Hormuz matters so much in the Iran war' (BBC News, 8 April 2026) https://www.bbc.com/news/articles/c78n6p09pzno accessed 5 May 2026.) 2, 10 17.

be complicated.[11] In addition, legal approaches to the protection of critical maritime infrastructure have faced criticism for insufficiently addressing the legal complexity, transnational character and geophysical conditions associated with subsea infrastructure in the marine environment.[12] The United Nations General Assembly has also emphasised the importance of international cooperation at global, regional and bilateral levels in addressing threats to maritime security and critical infrastructure at sea.[13]

The Baltic Sea constitutes a particularly relevant case context in this regard. The region contains a high concentration of cross-border maritime infrastructure and is one of the world's most intensively used maritime regions.[14] At the same time, the Baltic Sea is geographically and environmentally unique, characterised by shallow waters and sensitive marine ecosystems, factors which contribute to both the strategic importance and the vulnerability of subsea infrastructure located in the area. The cross-border and jurisdictionally fragmented nature of infrastructure in the Baltic Sea further complicates questions relating to its protection and governance. Recent incidents in the region have therefore highlighted not only the physical vulnerability of such infrastructure, but also the legal and jurisdictional challenges associated with its protection and governance.

The international legal framework governing maritime infrastructure is primarily established through the 1982 United Nations Convention on the Law of the Sea (UNCLOS).[15] Known as the "constitution for the oceans",[16] UNCLOS constitutes the central legal framework governing maritime zones, jurisdiction and the laying and protection of cables and pipelines. While UNCLOS provides a comprehensive framework governing all matters of the oceans, questions have nevertheless been raised regarding whether its structure of jurisdiction and enforcement is capable of addressing contemporary

[11] Rainer Lagoni 'Pipelines', Max Planck Encyclopedia of Public International Law (Oxford University Press April 2011) [17]. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e975; Daniel Runde, Erin Murphy and Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* (Center for Strategic and International Studies, August 2024) 2 https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf?VersionId=hn4OBAvGOF.c3WSZD9uJo6mGJviXZJWh accessed 13 April 2026.

[12] Bueger and Liebetrau (n 3) 6.

[13] United Nations General Assembly, 'Oceans and the Law of the Sea' (11 December 2023) UN Doc A/RES/78/69, [125]

[14] Peter Ehlers, 'Baltic Sea' in *Max Planck Encyclopedia of Public International Law* (Oxford University Press online, February 2014) https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1252?rskey=6cAxs6&result=8&prd=OPIL# accessed 16 April 2026.

[15] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 397.

[16] Henrik Ringbom, 'New Threats-Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Submarine Infrastructure in the Baltic Sea' (2025) 56 Ocean Development & International Law 390, 394.

threats to critical subsea infrastructure, particularly in maritime areas beyond territorial seas.[17]

The European Union has in recent years developed a broader resilience-oriented framework aimed at strengthening the protection of critical infrastructure. The framework, consisting of the Critical Entities Resilience Directive (CER)[18] and the Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2),[19] establish obligations relating to risk management, resilience, cybersecurity and incident response, while the EU Action Plan on Cable Security[20] sets out broader policy objectives and coordinated measures concerning the protection of subsea infrastructure and cross-border cooperation.

Against the background of recent incidents in the Baltic Sea, questions arise concerning the extent to which the UNCLOS regime governing submarine cables and pipelines is capable of addressing contemporary threats affecting critical subsea infrastructure, and whether the EU resilience framework contributes to strengthening the governance, resilience and protection of such infrastructure.

1.2 Purpose and Research Questions

This thesis aims to examine the extent to which the EU resilience framework, particularly the CER and NIS2 Directives, complements the UNCLOS regime's governance of critical subsea infrastructure in terms of cables and pipelines, in relation to contemporary threats in the Baltic Sea. To achieve this purpose, the following research questions will be examined:

- What legal framework does UNCLOS establish for submarine cables and pipelines and what structural limitations does it present for their protection?

- How do the CER and NIS2 Directives regulate critical subsea infrastructure and to what extent do they complement the UNCLOS regime in strengthening its governance, resilience and protection within the EU?

[17] See for example Hernandez-Benito (n 2) and Heintschel Von Heinegg, (n 8).

[18] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on resilience of critical entities and repealing Council Directive 2008/114/EC, (CER).

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L 330/80 (NIS2).

[20] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security* JOIN (2025) 9 final.

1.3 Delimitations

In order to maintain a clear and manageable scope and ensure a focus on aspects relevant to the purpose of this thesis, a number of delimitations have been made. The scope is geographically limited to the Baltic Sea region, which serves as the main case context due to its high concentration of cross-border subsea infrastructure and the recent incidents affecting such infrastructure. The analysis is limited to the legal dimensions of critical subsea infrastructure, specifically cables and pipelines, and does not engage with any technical or engineering aspects. Other forms of maritime infrastructure are referred to only where relevant for context or comparison.

From a legal perspective, the thesis focuses on the regulatory framework established by EU law, in particular the CER and NIS2 Directives, as well as relevant rules of public international law, primarily UNCLOS. The analysis of UNCLOS is limited to provisions relevant to the protection of subsea infrastructure in the Baltic Sea context. Consequently, certain maritime regimes under UNCLOS, such as those relating to archipelagic States, internal waters and the contiguous zone, are not examined. The thesis further excludes questions of private maritime law and does not analyse domestic law, despite its relevance for the implementation of EU legislation. The analysis is also limited to the regulatory framework applicable in peacetime and does not address the law of armed conflict or military operations at sea.

Although subsea infrastructure is closely connected to environmental protection and maritime safety, related international and regional regulatory frameworks fall outside the scope of this thesis. This includes environmental protection regimes such as the Helsinki Convention,[21] MARPOL[22] and the Marine Strategy Framework Directive[23], as well as maritime safety and security instruments adopted within the framework of the International Maritime Organization (IMO), including conventions and guidelines concerning navigational safety and ship security. While they may affect the operation, safety and environmental governance of subsea infrastructure, they mainly regulate vessels, navigational safety, shipping, port facilities and offshore platforms, rather than the governance and resilience of cables and pipelines. Maritime cybersecurity initiatives within the IMO framework are also omitted for the same reason.

While recent soft-law initiatives, including the 2024 Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures, are

[21] Convention on the Protection of the Marine Environment of the Baltic Sea Area (adopted 9 April 1992, entered into force 17 January 2000) 1507 UNTS 167.

[22] International Convention for the Protection of Pollution from Ships (adopted 2 November 1973, entered into force 2 October 1983) 1340 UNTS 184, as modified by the Protocol of 1978 relating thereto.

[23] Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive) [2008] OJ L 164/19.

relevant to the broader policy development concerning subsea infrastructure protection within the EU, they are not examined in detail. The EU Maritime Security Strategy is referred to where relevant as contextual background, whereas the EU Action Plan is used more extensively due to its specific focus on subsea infrastructure resilience and protection.

The definition of 'critical infrastructure' has been criticised in legal scholarship for being too expansive, abstract and policy driven, reflecting political assessments regarding what is considered societally essential rather than purely technical criteria.[24] This thesis will however not engage with this conceptual discussion and instead adopts the functional understanding reflected in the EU resilience framework.

1.4 Methodology and Materials

In order to analyse the legal framework governing the resilience and protection of critical subsea infrastructure under UNCLOS and EU law, the thesis applies a legal dogmatic method combined with methods of treaty interpretation and EU legal methodology.

The legal dogmatic method aims at analysing and establishing the law as it exists, de *lege lata*, through interpretations of legal sources holding authority.[25] While this is a commonly accepted aspect of the legal dogmatic method among scholars, the scope of the method regarding the types of argument it uses, is debated. It has been argued that the method merely encompasses arguments *de lege lata*, giving the method a purely descriptive role of the legal situation and thus leaving out any arguments of an analytical nature.[26] A more common view today is however, that discussions regarding how the law should be, *de lege feranda*, also fall within the scope of the legal dogmatic method. Scholars thus argue that the method allows for a more free and critically oriented approach, capable of problematising the state of the law and proposing solutions to legal issues that appear unresolved.[27] While the modern view of the scope of the method argues that *de lege feranda* reasoning may be included as the arguments constitute a development of the analysis, it is noted that arguments of a more legal-political character shall be avoided in the legal dogmatic method.[28]

---

[24] See for example Bueger and Liebetrau (n 3) 2.

[25] Claes Sandgren, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation* (4th edn, Norstedts Juridik 2018) 49–50; Mattias Hjertstedt, 'Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt' in Ruth Mannelqvist, Staffan Ingmanson and Carin Ulander-Wänman (eds), *Festskrift till Örjan Edström* (Juridiska institutionen, Umeå universitet 2019) 165, 166–167.

[26] Nils Jareborg, 'Rättsdogmatik som vetenskap' (2004) *SvJT 1,* 4

[27] Hjertstedt (n 25) 167; Jan Kleineman, 'Rättsdogmatisk metod' in Maria Nääv and Mauro Zamboni (eds), Juridisk metodlära (2nd edn, Studentlitteratur 2018) 21, 35–36.

[28] Sandgren (n 25) 45-49.

The analysis of this thesis is primarily conducted *de lege lata*, as it focuses on identifying and interpreting the existing legal framework governing the protection and resilience of critical subsea infrastructure under UNCLOS and EU law. However, in line with the broader understanding of the legal dogmatic method, the thesis also adopts certain *de lege feranda* elements to the degree that the analysis critically evaluates structural limitations, governance gaps and unresolved legal issues within the current framework. Such reasoning is intended to develop the analysis of existing law and assess the extent to which the EU resilience framework may complement the shortcomings within the UNCLOS regime, rather than to advance broader legal-political arguments.

Interpretation of treaty provisions is guided by the general rule of interpretation set out in Article 31(1) of the Vienna Convention on the Law of Treaties (VCLT),[29] which require treaties to be "interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty, in their context and in the light of its object and purpose". In accordance with Article 31(2), the context of the treaty is established through its text, including its preamble and annexes, as well as other relevant instruments or rules of international law between the parties. Where appropriate, supplementary means of interpretation, including preparatory works and the circumstances surrounding the treaty's conclusion, may also be utilised in accordance with Article 32 VCLT.

In light of the evolving nature of the threats against subsea infrastructure, the thesis additionally adopts a dynamic approach to the interpretation of relevant UNCLOS provisions, as advocated for by Henrik Ringbom and Alexander Lott.[30] Similarly, the International Court of Justice (ICJ) noted in *Costa Rica v. Nicaragua*, that it should be presumed that a treaty "that has been entered into for a very long period or is of 'continuing duration'" was intended by the parties to have terms of an evolving meaning.[31]

The EU legal methodology searches for guidance from the Court of Justice of the European Union (CJEU), which applies a wide range of interpretation methods, but most commonly relies on a teleological interpretation of the law.[32] Under this approach, a provision of EU law is not to be understood solely according to its wording, but also in light of its context and underly-

[29] Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331.

[30] Henrik Ringbom and Alexander Lott 'Sabotage of Critical Offshore Infrastructure: A Case Study of the Balticconnector Incident' in Alexander Lott (ed), *Maritime Security Law in Hybrid Warfare* (Brill 2024) 161-162.

[31] *Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (Judgement) [2009] ICJ Rep 213 [66].

[32] Jane Reichel, 'EU-rättslig metod', in: Maria Nääv and Mauro Zamboni (eds), *Juridisk metodlära* (2nd edn, Studentlitteratur 2018) 122.

ing objectives.[33] To facilitate such an approach, a systematic interpretation will be used, whereby legal provisions are understood in relation to the broader structure of the legal framework in which they operate. Rudolf Streinz uses the assumption that legal frameworks constitute an "orderly and meaningful system", and notes that systematic interpretation seeks to ascertain the function of a provision within the broader legal framework, thereby arguing that a systematic interpretation actually falls within the scope of a teleological interpretation.[34] The provisions of CER and NIS2 Directives, as well as other relevant EU instruments, will therefore be analysed in accordance with the CJEU's teleological method of interpretation and understood in a systematic manner, in the light of the broader legal framework to which they belong.

Given that the thesis examines the relationship between the EU resilience framework and UNCLOS, the analysis proceeds from the understanding that EU law and public international law do not operate in isolation from one another but frequently interact within interconnected and overlapping legal contexts. The CJEU regularly takes international law into account as a part of the EU legal context, while regulatory issues increasingly involve overlapping legal regimes operating simultaneously at international, EU and national levels.[35] All EU Member States are parties to UNCLOS as well as the EU itself, participating as an international organization pursuant to Annex IX. Accordingly, the Union and its members are bound by the Convention under the principle of *pacta sunt servanda*, codified in Article 26 of the Vienna Convention on the Law of Treaties and the Convention therefore forms part of the broader legal context within which the CER and NIS2 Directives operate, thus the EU framework should be understood consistently with the Union's obligations under UNCLOS.

A part of this thesis concerns the field of public international law. The authoritative enumeration of the recognised and accepted sources of international law is found in Article 38(1) Statute of International Court of Justice. The primary sources of law are international conventions, international custom and general principles of law,[36] Secondary sources such as "judicial

[33] C-292/82 *Merck Hauptzollamt Hamburg-Jonas* [1983] ECR 3781, para 12; Jörgen Hettne and Ida Otken Eriksson 'EU-rättsliga tolkningsmetoder' in Jörgen Hettne and Ida Otken Eriksson (eds), *EU-rättslig metod*: *Teori och genomslag i svensk rättstillämpning* (2nd edn, Norstedts Juridik 2011), 159.

[34] Rudolf Streinz 'Interpretation and Development of EU Primary Law' in Karl Riesenhuber (ed.) *European Legal Methodology (2nd* edn, Intersentia 2021) 157, 172.

[35] Christina Eckes, 'European Union Legal Methods – Moving Away from Integration' in Ulla Neergaard and Ruth Nielsen (eds), *European Legal Method – Towards a New European Legal Realism?* (DJØF Publishing 2013) 163, 171-172.

[36] Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) art 38(1)(a-c).

decisions and the teaching of the most highly qualified publicists" are to be used as subsidiary means for the determination of rules of law.[37]

The United Nations Convention on the Law of the Sea (UNCLOS) is a central legal source for this thesis as it is the main framework for all questions regarding the seas and oceans and establishes the primary international regime for submarine cables and pipelines. Its authority on the subject is additionally enhanced as both the ILC and the ICJ have affirmed that several of its provisions reflect customary international law, therefore also binding non-parties to its provisions.[38]

The thesis relies primarily on treaty law, policy documents and academic literature. In order to fully comprehend the context of the relevant provisions, subsidiary sources, including reports and doctrinal discussions, will also be used. The use of case law is limited due to the relative absence of judicial decisions directly addressing the protection of subsea infrastructure. The issues affecting cables and pipelines, are recent in nature and have not been the subject to legal proceedings in a substantial way. Therefore, the analysis focuses on the interpretation of relevant legal frameworks, in particular UNCLOS and the EU Directives of CER and NIS2, as well as the policy EU Action Plan on cable security, in the light of the recent incidents in the Baltic Sea area.

This thesis also accounts for soft law instruments and legally non-binding measures, including the EU Action Plan on Cable Security and Commission guidance documents. Although such instruments do not constitute binding legal sources, they may nevertheless provide insight into the Union's policy objectives, strategic priorities and practical approach to resilience and cable security.[39] Bruno de Witte contends that an analysis of EU law should not be confined solely to formally binding legal norms but should also consider institutional practices and instruments that influence the shaping and implementation of EU law. De Witte further emphasises that such a contextual approach may even be necessary for certain research questions.[40] In a similar vein, Johannes Köndgen and Oliver Mörsdorf has noted that Commission communications, guidelines and action plans, despite lacking binding force, may still influence the interpretation, implementation and practical

[37] Statute of the ICJ (n 37) art 38(1)(d).

[38] *North Sea Continental Shelf Cases* (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) [1969] ICJ Rep 3, para 65; *Territorial and Maritime Dispute* (Nicaragua v Colombia) (Judgement) [2012] ICJ Rep 624 para 118; *Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea* (Nicaragua v Colombia) [2022] ICJ Rep 266, [57]; Tara Davenport, 'Intentional Damage to Submarine Cable Systems by States' (Aegis Series Paper No 2305, Hoover Institution 2023) 2-3.

[39] See for example C-410/09 *Polska Telefonia Cyfrowa*, EU:C:2011:294, paras 30-35.

[40] Bruno de Witte 'Legal Methods for the Study of EU institutional Practice' [2022] 18(4) ECLR, 637, 638-639.

development of EU law.[41] By applying a broader perspective and analysing policy-oriented instruments alongside binding legislation, the present thesis thus seeks to provide a more comprehensive understanding of the legal framework surrounding the resilience and protection of critical subsea infrastructure.

Earlier scholarly contributions, including the work of Wolff Heintschel von Heinegg from 2013,[42] are also used where relevant. Although the legal and strategic context surrounding subsea infrastructure has developed significantly in recent years, earlier scholarship remains valuable for understanding the historical development of the field.

Given the evolving and relatively underexplored nature of legal questions relating to the protection of critical subsea infrastructure, chapter two provides a broader contextual discussion concerning the strategic significance, vulnerabilities and regional characteristics of such infrastructure in the Baltic Sea region. This context is intended to facilitate the later legal analysis by situating the examined legal frameworks within the practical and geopolitical circumstances in which they operate.

1.5 Research Overview

UNCLOS has been extensively discussed in the academic literature, but recent incidents affecting subsea infrastructure have generated increasing scholarly attention to the protection and governance of submarine cables and pipelines under international law. Existing research has examined issues relating to maritime jurisdiction, submarine cable protection, enforcement limitations and hybrid threats affecting maritime infrastructure. Scholars such as Robert Beckman, Tara Davenport, Douglas Burnett, Zhen Sun, Tamsin Philipa Paige, Rob McLaughlin and Douglas Guilfoyle have particularly addressed the legal regime governing submarine cables and questions relating to the protection of subsea infrastructure under UNCLOS.

Following the Nord Stream sabotage and subsequent incidents in the Baltic Sea, the literature has also increasingly addressed broader governance and security implications of critical subsea infrastructure in the Baltic Sea region. In this regard, authors such as David Langlet, Henrik Ringbom, Christian Bueger and Tobias Liebetrau, have examined questions relating to maritime governance fragmentation, hybrid threats and structural challenges concerning the protection of maritime infrastructure in the Baltic Sea context.

[41] Johannes Köndgen and Oliver Mörsdorf 'The Sources of European Private Law' in Karl Riesenhuber (ed.) *European Legal Methodology 2nd* edn, Intersentia 2021) 117, 152-154.

[42] Heintschel von Heinegg (n 8).

On the topic of EU law, Marcos Julien Alexopoulos, Arto Niemi, Bartosz Skobiej and Frank Sill Torres have examined the EU Resilience framework's function in regard to the maritime area, while Marie Becker has examined the implementation of the EU's critical infrastructure protection framework in the Baltic Sea region specifically.

Limited attention has however been paid to how the EU resilience framework may complement the structural limitations of the UNCLOS regime in relation to subsea infrastructure protection, particularly in the Baltic Sea context. This thesis therefore seeks to contribute to that discussion by examining the interaction between UNCLOS and the EU resilience framework from that perspective.

1.6 Outline

The thesis will henceforth have the following structure. Chapter two introduces the concept of critical subsea infrastructure in the Baltic Sea context, with particular focus on cables and pipelines, their vulnerabilities and the legal and practical challenges associated with their protection.

Chapter three examines the United Nations Convention on the Law of the Sea (UNCLOS), which constitutes the principal public international law framework governing subsea infrastructure. Particular attention is given to the maritime zones established under UNCLOS, the allocation of jurisdiction between States and the structural limitations of the Convention in relation to the protection of subsea infrastructure against contemporary threats.

Chapter four examines the EU resilience framework relevant to infrastructure protection. The chapter focuses primarily on the CER and NIS2 Directives and analyses how the EU approaches the physical and cybersecurity dimensions of critical infrastructure protection. The EU Action Plan on Cable Security is also discussed as a complementary policy instrument within the broader EU framework.

Finally, chapter five contains the analytical discussion of the thesis, where the research questions are examined and answered through a comparative analysis of UNCLOS and the EU resilience framework. The thesis concludes in chapter six with a summary of the main findings and conclusions of the study.

2 The Legal and Strategic Context of Critical Subsea Infrastructure in the Baltic Sea

Due to the technical, transnational and interdisciplinary nature of submarine cables and pipelines, a contextual understanding of the Baltic Sea environment, the characteristics of such infrastructure and the risks affecting it is necessary in order to examine the legal frameworks governing them and the legal challenges associated with their protection.

While contemporary policy and security discussions increasingly refer to "subsea infrastructure", UNCLOS primarily uses the terminology "submarine cables and pipelines". Both terms are therefore used in this thesis depending on context.

2.1 Critical Subsea Infrastructure

Submarine cables and pipelines are central components of modern societies, enabling global communication through digital data transmissions and the transport of energy resources between States. Due to their importance for essential services and vital societal functions, they are commonly regarded as critical infrastructure within the EU. Disruptions affecting such infrastructure may therefore have significant societal and economic consequences. Submarine cables alone carry the vast majority of intercontinental internet traffic,[43] illustrating the extent to which modern societies depend on the stability and resilience of such infrastructure.

Subsea infrastructure is also inherently transnational and largely privately owned and operated.[44] Its protection therefore depends not only on national regulation but also on international cooperation and coordination between States and private actors.[45]

2.2 Risks, Vulnerabilities and Consequences

2.2.1 Risks and Vulnerabilities

Critical subsea infrastructure is exposed to a broad range of natural, human-induced and hybrid threats. Damage can arise unintentionally from ordinary maritime activities, such as anchor dragging and fishing activities, often caused by negligence or lack of awareness. At the same time the infrastruc-

[43] Bueger and Liebetrau (n 3) 1-2.
[44] Bueger and Liebetrau (n 3) 3.
[45] Lagoni (n 11) para 17; Runde, Murphy and Bryja (n 11) 2.

ture may be subject to intentional interference by criminal actors, terrorist groups or malicious States.[46]

The vulnerability of subsea infrastructure is closely linked to both its strategic importance and its placement on or beneath the seabed, where monitoring and protection are difficult. Increasing dependence on cable systems and cross-border energy infrastructure has increased the strategic significance of the seabed and the potential consequences of disruptions affecting such infrastructure.[47]

The distinction between accidental damage and intentional interference has become increasingly complex due to the growing prevalence of hybrid or grey-zone activities, particularly in incidents involving the cutting of submarine cables. Such operations are often designed to remain below the threshold of armed conflict[48] and are obscured or presented as accidents. The ambiguity surrounding the origin, intent and nature of such incidents allows plausible deniability for suspected State actors, thereby complicating the attribution of responsibility and the practical enforcement of legal obligations relating to subsea infrastructure protection.[49]

Technological developments and increasing digitalisation have also introduced a cyber dimension to the threats facing such infrastructure. Cyberattacks targeting interconnected systems may cause indirect and cross-sectoral consequences extending beyond the originally targeted infrastructure, as illustrated by the NotPetya cyberattacks.[50]

2.2.2 Consequences

Disruptions affecting subsea infrastructure may have significant societal, economic and environmental consequences. The loss of connectivity may disrupt financial transactions, government functions, communication systems and military operations, while damage to energy infrastructure specifically may affect energy supply and broader economic stability.[51]

Damage to subsea infrastructure can also result in prolonged and financially costly recovery periods. Repairs often require specialised vessels, and limited repair capacity may delay restoration and extend disruptions affecting connectivity and energy transmission.[52] Damage to pipelines in particular,

[46] Bueger & Liebetrau (n 3) 4.
[47] Bueger & Liebetrau (n 3) 4; Heintschel von Heinegg (n 8) 293-295;
[48] 'Armed attack' understood in accordance with the UN Charter Article 51; Juraj Majcin, 'Battle of the Baltic: Safeguarding Critical Undersea Infrastructure' (European Policy Centre, 22 April 2025) https://www.epc.eu/publication/Battle-of-the-Baltic-Safeguarding-critical-undersea-infrastructure-645780/ accessed 20 April 2026.
[49] Bueger and Liebetrau (n 3) 5; Majcin (n 49).
[50] Bueger and Liebetreau (n 3) 4.
[51] Heintschel von Heinegg (n 8) 293.
[52] European Commission, Joint Research Centre (n 1).

may also have serious environmental consequences. The scale of such risks was demonstrated by the explosions affecting the Nord Stream pipelines in 2022, which resulted in one of the largest recorded releases of methane in history, despite no gas being transported through the pipelines at the time.[53]

2.3 The Baltic Sea as a case context

2.3.1 Regional Characteristics

The Baltic Sea is bordered by nine coastal States, namely Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden. All of these States, with the exception of Russia, are members of both the EU and NATO.[54] Their shared geographical position and long-standing regional cooperation have contributed to extensive coordination concerning maritime governance in the region.[55]

The Baltic Sea is geographically and environmentally distinct. It is relatively shallow and characterised by brackish water and sensitive marine ecosystems. These conditions contribute both to the exposure and vulnerability of subsea infrastructure located on or beneath the seabed and to the environmental sensitivity of the region in the event of damage to such infrastructure.[56]

2.3.2 Jurisdictional Complexity

In jurisdictional terms, the Baltic Sea area is almost entirely divided into the surrounding Coastal States' territorial seas, EEZs and continental shelves under UNCLOS, leaving no remaining areas of high seas in the region. Most of the maritime boundaries have been determined through bilateral and trilateral agreements, resulting in an exceptionally high degree of clearly defined maritime delimitation in international comparison. This dense jurisdictional division is relevant for subsea infrastructure, which frequently extends across several maritime zones and national jurisdictions, thereby creating complex questions concerning jurisdiction and enforcement.[57]

---

[53] ILA Interim Report 2024, [57]; UN Environment Programme 'Pipeline blasts released record-shattering amount of methane: UNEP study' https://www.unep.org/news-and-stories/story/pipeline-blasts-released-record-shattering-amount-methane-unep-study (accessed 18 April 2026). The study suggests the emissions are comparable to the annual emissions of approximately 8 million cars.

[54] Peter Ehlers (n 12) [1].

[55] Ehlers (n 12) [1].

[56] Ehlers (n 12) [3]; Marko Joas, Henrik Ringbom and Nina Tynkkynen, 'The Baltic Sea and Global Environmental Change' in Paul G Harris (ed) *Routledge Handbook of Marine Governance and Global Environmental Change* (Routledge 2022) 196–197.

[57] Erik Franckx 'Regulatory Gaps in Baltic Sea Governance' in Henrik Ringbom (ed), *Regulatory Gaps in Baltic Sea Governance: Selected Issues* (Springer International Publishing 2018) 14, 15 and 19.

The Baltic Sea is one of the most heavily trafficked maritime regions globally and a majority of the vessels navigating the area are registered under the flags of states that are not bordering the Baltic Sea. As a result, incidents affecting subsea infrastructure frequently involves foreign vessels operating across several maritime zones and jurisdictions. This creates practical and legal challenges concerning jurisdiction and enforcement under UNCLOS.[58]

2.3.3 Recent Incidents in the Baltic Sea

In recent years, a series of incidents affecting subsea infrastructure in the Baltic Sea have attracted significant media attention and raised concern among the Baltic Sea coastal states regarding the vulnerability of such infrastructure. These incidents illustrate both the increasing frequency of disruptions and the complexity of responding to them in a maritime context characterised by overlapping jurisdictions and limited enforcement powers.

A significant early incident occurred in September 2022, when multiple explosions damaged the Nord Stream 1 and 2 gas pipelines on the seabed in the EEZs of Sweden and Denmark.[59] Separate investigations were initiated by Sweden, Denmark and Germany and although Swedish and Danish investigations were later discontinued due to a lack of jurisdiction or insufficient grounds for prosecution, Germany's investigation remains ongoing. The incident marked a turning point in the perception of risks relating to subsea infrastructure.[60]

In October 2023, the Balticconnector gas pipeline and several cables between Estonia and Finland were damaged in the EEZs and continental shelves of the two States after a cargo ship was suspected of having dragged its anchor along the seabed. Finnish authorities faced limitations in taking enforcement action against the suspected foreign vessel due to jurisdictional constraints as the ship did not enter the Finnish territorial sea.[61] Similar difficulties arose following incidents in 2024 involving the cutting of the cables BCS East West Interlink and C-Lion1 in the Swedish EEZ, where in-

[58] Ehlers (n 12) [9].

[59] International Law Association, 'Third Interim Report of the ILA Committee on Submarine Cables and Pipelines' (2024) [5].

[60] 'The Nord Stream Incident: Open Briefing' (Security Council Report, 26 August 2025) https://www.securitycouncilreport.org/whatsinblue/2025/08/the-nord-stream-incident-open-briefing-2.php accessed 25 April 2026; Åklagarmyndigheten, 'Åklagaren lägger ned den svenska förundersökningen om grovt sabotage mot Nord Stream' (7 February 2024), https://www.aklagare.se/for-media/pressmeddelanden/2024/februari/aklagaren-lagger-ned-den-svenska-forundersokningen-om-grovt-sabotage-mot-nord-stream/ accessed 24 April 2026.

[61] Henrik Ringbom and Alexander Lott, 'Sabotage of Critical Offshore Infrastructure: A Case Study of the Balticconnector Incident' in Alexander Lott (ed), *Maritime Security Law in Hybrid Warfare* (Brill, 2024) 155.

vestigations also did not result in formal legal proceedings despite suspicions of deliberate interference.[62]

Further incidents involving damage to subsea infrastructure, including the damage caused to the Estlink 2 cables in the Finnish EEZs by the tanker *Eagle S* in 2024 as well as the *Vezhen* incident in Sweden's EEZ in 2025, continued to demonstrate both the recurring nature of such disruptions and the legal complexities associated with incidents occurring outside territorial waters. In certain cases, such as the *Eagle S* incident, coastal State authorities were able to take more extensive measures once the vessel entered territorial waters, whereas other incidents, including the *Vezhen* case, showed the legal difficulties associated with establishing criminal responsibility despite confirmed damage to subsea infrastructure.[63]

2.3.4 Regional Cooperation and Security Responses

The Baltic Sea is often described as a prime example of multilevel and network-based governance, involving the interaction of EU law, regional cooperation, national regulation and local actors.[64]

Regional cooperation in the Baltic Sea has long been institutionalised through frameworks such as the Helsinki Convention. While primarily focused on environmental protection, the Helsinki Convention demonstrates the existence of established mechanisms for regional cooperation and coordination in relation to transboundary maritime risks.[65] EU action in the Baltic Sea furthermore takes place alongside this broader framework of regional cooperation, as the EU itself is a Party to the Helsinki Convention.[66]

2.4 Concluding Observations

The protection of submarine cables and pipelines involves legal challenges extending beyond purely technical or security-related concerns, as illustrated by the present situation in the Baltic Sea. The transnational and interconnected nature of such infrastructure, in combination with the jurisdictional division of the Baltic Sea into multiple maritime zones, creates complex questions regarding governance, enforcement, coordination and responsibility. These characteristics increase the importance of legal frameworks and provisions capable of addressing both the jurisdictional structure governing

[62] Ringbom (n 16) 391; Alexander Lott, 'The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident' (Lieber Institute for Law and Land Warfare, 26 November 2024) https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/ accessed 25 April 2026.

[63] Ringbom (n 16) 391-392.

[64] Joas, Ringbom and Tynkkynen, (n 57) 196 and 198.

[65] See the Helsinki Convention (n 21).

[66] Helsinki Commission (HELCOM), 'Contracting Parties' https://helcom.fi/about-us/contracting-parties/ accessed 20 April 2026.

maritime areas and the broader resilience and coordination challenges associated with contemporary threats affecting critical subsea infrastructure.

The contextual characteristics and recent incidents discussed above illustrate why the protection of cables and pipelines increasingly raises questions concerning jurisdiction, governance, enforcement and resilience. Against this background, the following chapters examine the legal framework governing such infrastructure.

3 Subsea Infrastructure under Public International Law

3.1 The Law of the Sea Framework

UNCLOS is the most comprehensive and up-to-date law of the sea framework governing maritime infrastructure and thus constitutes the primary legal framework for submarine cables and pipelines. UNCLOS has 169 parties, including the Baltic coastal States as well as the European Union. It is widely recognised that several of its provisions reflect customary international law, particularly those relating to the exclusive economic zone, the continental shelf and the high seas, thus representing binding law even for non-party States.[67]

The current legal framework governing subsea infrastructure builds upon earlier developments in international law. Following the laying of the first transatlantic cables, States adopted the 1884 Convention for the Protection of Submarine Telegraph Cables,[68] which introduced principles concerning the protection of submarine cables beyond territorial waters, including obligations relating to criminalisation and flag state jurisdiction. While the 1884 Convention remains in force for a number of States, its practical relevance is limited as it was originally designed for telegraph cables.[69] The rules it established, however, continued to influence the legal framework governing subsea infrastructure. The International Law Commission (ILC) incorporated several of the Convention's principles into its 1956 Draft Articles on the Law of the Sea, considering them to constitute essential principles of international law.[70] These principles were subsequently incorporated into later instruments, including the 1958 Geneva Convention on the High Seas[71] and ultimately UNCLOS.

UNCLOS governs submarine cables and pipelines through a range of provisions concerning maritime jurisdiction, the laying and maintenance of subsea infrastructure and obligations relating to its protection. As subsea infrastructure typically extends across multiple maritime zones, the applicable rights, obligations and enforcement powers vary depending on where the infrastructure is located.[72] Therefore, the following sections examine how

[67] See the *North Sea Continental Shelf Cases* (n 39); Davenport (n 39) p. 2–3; Henrik Ringbom (n 16) 390, 394.

[68] Convention for the Protection of Submarine Telegraph Cables (adopted 14 March 1884, entered into force 1 May 1888) 24 Stat 989.

[69] Heintschel von Heinegg (n 8) 297.

[70] See Summary Records of the Seventh Session, [1955] 1 Y.B. International Law Commission 20–21, U.N. Doc. A/CN.4/Ser.A/1955.

[71] Convention on the High Seas (adopted 29 April 1958, entered into force 30 September 1963) 450 UNTS 11.

[72] Bueger & Liebetrau (n 3) 2.

the UNCLOS framework regulates subsea infrastructure and how its jurisdictional structure affects the protection and enforcement of such infrastructure in practice.

3.2 Maritime Zones under UNCLOS

The legal regime governing subsea infrastructure under UNCLOS is shaped by the Convention's system of maritime zones. Rights, enforcement powers and regulatory authority relating to submarine cables and pipelines vary depending on the maritime zone in which the infrastructure is located or affected. The following sections therefore examine the territorial sea, the exclusive economic zone, the continental shelf and the high seas as the main zones relevant to maritime infrastructure in the Baltic Sea. The maritime zones discussed below are illustrated in this thesis' Annex I.

3.2.1 Territorial Sea

The territorial sea extends up to 12 nautical miles from a coastal State's baselines, usually measured from the low-water line along the coast.[73] Within this area, the coastal State's sovereignty extends beyond its land territory, encompassing the waters, seabed, subsoil as well as the air space over it.[74] This sovereignty is however limited by the right of innocent passage, established in UNCLOS Article 17 and enjoyed by ships of all States. According to Article 18, passage constitutes navigation through the territorial sea for the purpose of traversing it without entering internal waters or proceeding to or from a port. The passage shall be continuous and expeditious, and stopping or anchoring is only permitted if it is incidental to ordinary navigation, deemed necessary by force majeure or undertaken for the purpose of assisting persons, ships or aircrafts in danger or distress. For the passage to qualify as innocent, it must not be prejudicial to the peace, good order or security of the coastal State and shall be performed in accordance with UNCLOS and other provisions in international law.[75] UNCLOS permits coastal States to take the necessary measures in their territorial seas to prevent passage that is not innocent through Article 25.

Within their territorial seas, coastal States may adopt laws and regulations governing innocent passage in accordance with UNCLOS and other rules of international law. Coastal States are explicitly permitted to regulate matters such as navigational safety, maritime traffic, environmental protection and the protection of submarine cables and pipelines, with which all foreign ships exercising the right of innocent passage must comply.[76] Coastal States' authority to adopt such regulation reflects the relatively extensive prescriptive authority they possess within their territorial seas, including the

[73] UNCLOS Articles 3 and 5.
[74] UNCLOS Article 2(1-2).
[75] UNCLOS Article 19(1).
[76] UNCLOS Articles 21(1)(a, c, d, f) and 21(4).

ability to adopt regulation aimed at preventing damage to subsea infrastructure.[77]

Compared to other maritime zones under UNCLOS, coastal States possess significantly broader enforcement and regulatory powers within the territorial sea in relation to the protection of submarine cables and pipelines.

3.2.2 EEZ

Beyond and adjacent to the territorial sea, the exclusive economic zone (EEZ) extends up to 200 nautical miles from the baselines used in the measurement of the territorial sea, as stipulated by UNCLOS Articles 55 and 57. Within the EEZ, the coastal State does not exercise full sovereignty, but instead holds sovereign rights specifically attributed under UNCLOS. These rights include the exploration, exploitation, conservation and management of natural resources of the waters, seabed and subsoil, as well as other economic uses of the zone.[78]

At the same time, other States still retain certain high seas freedoms within the EEZ, including navigation, overflight and the laying of submarine cables and pipelines.[79] According to Article 58(1) UNCLOS, the high seas regime and other pertinent rules of international law continue to apply within the EEZ as long as they are compatible with the specific legal regime governing the zone. The exercise of the rights and freedoms of both the coastal State and other States is furthermore governed by a mutual obligation of due regard for each other's rights and duties.[80] The EEZ is therefore regarded as a *sui generis* maritime zone,[81] combining both elements of coastal State jurisdiction and high seas freedoms.[82] This balance becomes especially important in the Baltic Sea, where recent incidents have highlighted the difficulties coastal States may face when responding to disruptive activities conducted by foreign-flagged vessels within the EEZ. Coastal State enforcement powers are thus more limited in relation to incidents affecting subsea infrastructure than within territorial waters.

3.2.3 Continental Shelf

The seabed and subsoil beyond a coastal State's territorial sea constitute the continental shelf. This submarine area represents the natural prolongation of the State's land territory and extends to the outer edge of the continental margin. Where the continental margin does not extend to 200 nautical miles

[77] International Bar Association, *Report of the Task Force on Extraterritorial Jurisdiction* (2008) 7-8 <https://www.ibanet.org/MediaHandler?id=ECF39839-A217-4B3D-8106-DAB716B34F1E> accessed 10 March 2026.

[78] UNCLOS Article 56(1)(a).

[79] UNCLOS Article 58; The high sea freedoms in UNCLOS Article 87

[80] UNCLOS Articles 56(2) & 58(3).

[81] Sui generis ('Of its own kind').

[82] UNCLOS Articles 55-58; Yoshifumi Tanaka, *the International Law of the Sea* (4th edn. Cambridge University Press) p. 161-162.

from the baselines, the continental shelf nevertheless extends to that distance.[83] In the Baltic Sea, the continental shelves of the coastal States largely overlap geographically with the seabed beneath their respective EEZs.[84]

Coastal States exercise sovereign rights over the continental shelf for the purpose of exploring and exploiting its natural resources. These rights arise automatically by virtue of the State's sovereignty over their land territory and do not depend on occupation or formal proclamation and exist *ipso facto* and *ab initio*.[85] The rights of the coastal State, however, only relate to the seabed and subsoil and do not affect the legal status of superjacent waters or air space. The exercise of coastal State rights over the continental shelf must furthermore respect the rights and freedoms of other States and must not unjustifiably interfere with activities such as navigation or other uses of the sea recognised under UNCLOS.[86]

Article 79 UNCLOS provides that all States are entitled to lay submarine cables and pipelines on the continental shelf, subject to certain rights of the coastal State. The coastal State may not impede the laying or maintenance of cables and pipelines, however, it retains certain rights, such as the right to take reasonable measures for the exploration and exploitation of natural resources, as well as the right to consent to the delineation of the course of pipelines. States laying cables or pipelines must likewise have due regard to such infrastructure already in position, meaning that the laying of new infrastructure must not interfere with existing cables or pipelines or prejudice their maintenance and repair.

3.2.4 High Seas

The high seas regime is residual and applies to all maritime areas that do not form part of the EEZ, territorial sea, internal waters or archipelagic waters of any State under UNCLOS Article 86. The high seas are open to all States and include freedoms such as navigation, overflight and the laying of submarine cables and pipelines.[87] These freedoms are, however, not absolute and must be exercised with due regard for the rights and interests of other States on the high seas in accordance with UNCLOS.[88] The regime reflects the principle of *res communis*, under which the high seas are not subject to the sovereignty or exclusive jurisdiction of any State but remain open to all States, whether coastal or landlocked.[89]

---

[83] UNCLOS Article 76(1).

[84] Ringbom (n 16) 401.

[85] UNCLOS Article 77(3); North Sea Continental Shelf Cases (n 39), p 22, para 19; ipso facto ('by the fact itself'), ab initio ('from the beginning'); Tanaka (n 84) p. 187.

[86] UNCLOS Article 78(1-2).

[87] UNCLOS Article 87(1)(a)-(c).

[88] UNCLOS Article 87(2).

[89] UNCLOS Articles 87 and 89.

Although the Baltic Sea is almost entirely covered by territorial seas and EEZs, high seas freedoms remain relevant through Article 58 UNCLOS, which extends certain freedoms under Article 87 to the EEZ. Similarly, Article 112 recognises the right of all States to lay cables and pipelines on the bed of the high seas beyond the continental shelf.

3.3 Protection of Subsea Infrastructure and Enforcement Competences

UNCLOS also contains provisions concerning the protection of submarine cables and pipelines through criminalisation of damage, liability for damage caused and compensation in situations where damage has been avoided, in addition to provisions on the allocation of enforcement jurisdiction between States.

Article 113 requires States to provide that the breaking or injury of submarine cables or pipelines by a ship flying their flag, or by a person subject to their jurisdiction, constitutes a punishable offence under national law. This applies both to wilful conduct and conduct resulting from culpable negligence. An exception is provided where damage results from actions taken for the purpose of saving life or ships at sea, provided that all necessary precautions have been taken.

UNCLOS additionally addresses liability and compensation in relation to damage to subsea infrastructure. Article 114 provides that persons responsible for damaging existing cables or pipelines in the course of laying or repairing another cable or pipeline are required to bear the cost of repairs. Article 115 additionally provides for compensation where fishing gear has been sacrificed in order to avoid damage to such infrastructure.

The enforcement of obligations relating to cables and pipelines in EEZs and on the continental shelves under UNCLOS is primarily based on the nationality principle and flag State jurisdiction. States primarily exercise jurisdiction over ships flying their flag and persons subject to their jurisdiction. UNCLOS does not establish a system of universal jurisdiction in relation to incidents affecting subsea infrastructure.[90] This allocation of jurisdiction is reflected in Article 97, which provides that in the event of a collision or other incident of navigation on the high seas, penal or disciplinary proceedings may only be instituted by the authorities of the flag State or the State of nationality of the persons concerned. As a result, obligations relating to submarine cables and pipelines, including those set out in Article 113, are enforced by the flag State in respect of ships flying its flag or persons subject to its jurisdiction. This means that enforcement action is, as a general rule,

[90] UNCLOS arts 92 and 94; Rene Jean Dupuy and Daniel Vignes, 'Submarine Cables and Pipelines' in Rene Jean Dupuy & Daniel Vignes (eds) *A Handbook on the New Law of the Sea*, vol. 2 (Brill/Nijhoff 1991) 977-988.

dependent on the State of nationality of the vessel or individual concerned. While UNCLOS contains certain enforcement mechanisms available to coastal State such as their right of hot pursuit of foreign ships under Article 111, such powers are connected to the coastal State's jurisdiction within internal waters and territorial seas. Consequently, this mechanism is of limited practical relevance in incidents affecting infrastructure outside territorial seas, where coastal State enforcement competences remain comparatively restricted.

3.4 Interpretations of UNCLOS in Relation to Subsea Infrastructure

Although UNCLOS establishes the principal legal framework governing submarine cables and pipelines, recent incidents in the Baltic Sea have prompted renewed discussions concerning how UNCLOS should be interpreted in relation to contemporary security threats and enforcement challenges.

While UNCLOS is generally understood as relying primarily on flag State jurisdiction in maritime areas beyond the territorial sea, recent scholarship has questioned whether such a rigid flag State-centred understanding fully reflects the broader structure and underlying principles of the Convention.

An assumption underlying UNCLOS, similar to most treaties, is that its parties will fulfil their obligations in good faith and the exercise of the rights, jurisdiction and freedoms provided in the Convention are to be exercised "in a manner which would not constitute an abuse of rights".[91] Furthermore, the Convention emphasises mutual understanding and cooperation between States, while paying due regard to State sovereignty and promoting international communication and the peaceful use of the seas and oceans.[92] Consequently, the broader object and purpose of UNCLOS support interpretations aimed at protecting subsea infrastructure against deliberate interference. The Convention does not appear to support an interpretation under which actors engaging in sabotage at sea could invoke the freedom of navigation as protection against investigation and accountability.[93]

Furthermore, the absence of explicit enforcement powers for coastal States against sabotage of subsea infrastructure does not necessarily imply that such powers are entirely excluded under UNCLOS, especially within the EEZ. That being said, the scope of such enforcement powers remains uncertain and constrained in practice due to the absence of explicit treaty provisions and proportionality requirements. Nevertheless, both ITLOS and arbitral tribunals have in certain circumstances indicated a willingness to justify

[91] UNCLOS, article 300.
[92] UNCLOS, preamble.
[93] Ringbom and Lott (n 30) 161; Ringbom (n 16) 404–405.

broader coastal State enforcement measures within the EEZ, even where such powers are not expressly provided for under UNCLOS.[94] Due to the Convention's object and purpose to establish a comprehensive and durable framework for the seas, a dynamic interpretation of UNCLOS has been advocated, especially with regard to the new types of challenges facing the law of the sea, which were not envisioned by the drafters of UNCLOS.[95]

International law mainly remains centred around the State as the principal creator, implementer and enforcer of legal obligations.[96] This is visible in the UNCLOS framework governing subsea infrastructure, where protection of infrastructure and legal enforcement primarily depends on the jurisdictional competences and political willingness of individual States. The transnational and interconnected nature of subsea infrastructure does not always align neatly with the zonal and jurisdiction based structure established under UNCLOS. It has been noted that such mismatches between regulatory structures and the systems they seek to govern may impede the effectiveness of regulatory efforts.[97]

3.5 Concluding Remarks

UNCLOS was primarily designed to regulate the allocation of maritime rights and jurisdiction and facilitate the coexistence of different maritime uses. UNCLOS will thus naturally not serve as a comprehensive framework for the protection of subsea infrastructure. Although the Convention establishes important rules concerning the laying, maintenance and protection of cables and pipelines, the applicable rights, obligations and enforcement powers relating to such infrastructure vary significantly depending on the maritime zone in which it is located.

As demonstrated throughout this chapter, coastal States possess comparatively broad regulatory and enforcement powers within the territorial sea, whereas their competences become considerably more limited within the EEZ and on the continental shelf, where the Convention continues to preserve important freedoms for other States, including navigation and the laying of submarine cables and pipelines. Recent incidents in the Baltic Sea further illustrates how the jurisdictional structure under UNCLOS may create practical and legal difficulties in relation to contemporary maritime threats. The Convention primarily relies on flag State jurisdiction, inter-State cooperation and due regard obligations and it provides a limited enforcement powers for coastal States beyond territorial waters, at least expressively.

---

[94] Ringbom (n 16) 404–405.

[95] Ringbom and Lott (n 30) 161-162.

[96] David Langlet 'Scale, space and delimitation in marine legal governance – Perspectives from the Baltic Sea' (2018) 98 *Marine Policy* 278, 280.

[97] Langlet (n 98) 284.

The transnational and interconnected nature of subsea infrastructure does not always correspond with the zonal structure established under UNCLOS. These structural characteristics thus help explain why questions concerning resilience, coordination and protection of critical subsea infrastructure have increasingly gained importance within regional frameworks such as the European Union.

4 The EU Resilience Framework

EU law plays a central role in establishing regulatory and coordination efforts for protection of subsea infrastructure in the Baltic Sea region, especially since all but one of the Baltic Sea coastal States are EU members. In response to increasing concerns regarding the vulnerability of critical infrastructure and growing threats against submarine cables and pipelines, the EU has adopted a broader resilience framework. Within the European Union, critical infrastructure broadly refers to assets, facilities, equipment, networks or systems, or any part thereof, that are necessary for the provision of essential services, which are crucial for maintaining vital societal functions, economic activities, public health and safety or the environment.[98]

Against this background, the following sections examine the main elements of the EU resilience framework relevant to subsea infrastructure protection, focusing on the CER and NIS2 Directives. A brief examination of the EU Action Plan on Cable Security will also be made as it functions as a complementary policy instrument within the broader framework.

4.1 The Critical Entities Resilience Directive (CER)

Earlier EU approaches to critical infrastructure protection have been criticised for their limited harmonisation and lack of transnational coordination, as Member States have tended to prioritise national approaches in sensitive security areas. Earlier EU instruments have been criticised for insufficiently addressing the maritime dimension, including infrastructure located beyond territorial waters.[99] The limited effectiveness of earlier EU instruments, in particular the European Critical Infrastructure Directive (ECI),[100] further highlighted these shortcomings.

Within the broader EU maritime security framework, the EU Maritime Security Strategy (EUMSS) identified underwater pipelines and seabed cables as part of the Union's critical maritime infrastructure and emphasised the importance of cross-border cooperation, information sharing and maritime risk management.[101]

---

[98] CER Article 2(4-5).

[99] Marie Becker, 'Transposing EU-legislation on critical infrastructure protection legal implementation performance in the Baltic Sea region' (2025) 50 *International Journal of Critical Infrastructure Protection* 100781, 9.

[100] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75; Becker (n 101) 1.

[101] Council of the European Union, European Union Maritime Security Strategy (Council of the European Union, 24 June 2014) 11205/14; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strat-

In response to these shortcomings and in light of recent developments affecting European maritime security, for example hybrid threats and attacks on critical infrastructure, the strategic importance of resilience frameworks at EU level has increased. This resulted in the adoption of the CER Directive in 2022, which entered into force in 2023, as a central instrument for strengthening the protection and resilience of critical entities. While the CER Directive builds upon earlier EU frameworks on critical infrastructure, it adopts a broader and more resilience-oriented approach.[102] As the identification of critical entities under the Directive is to be completed by the Member States by 17 July 2026, the framework is in a relatively early phase of implementation across the Union. [103]

4.1.1 Purpose, Scope and Key Concepts

Through the CER Directive, Member States are required to take measures aimed at enhancing the resilience of critical entities and ensuring their ability to provide services essential for the maintenance of vital societal functions or economic activities without obstruction within the internal market.[104]

The CER Directive is designed to operate alongside the NIS2 Directive, and its Article 1(2) explicitly excludes matters covered by the NIS2 Directive from its scope, while still requiring Member States to ensure that both instruments are implemented in a coordinated manner. Article 3 CER furthermore establishes a minimum harmonisation framework and hence does not prevent Member States from adopting or maintaining national law providing a higher level of resilience than the Directive requires, provided that such measures are compatible with Union law.

4.1.2 Member State Obligations and Identification of Critical Entities

The competent authorities of each Member State shall conduct national risk assessments based on the non-exhaustive list of essential services in the sectors and subsectors set out in the CER directive. The purpose of these assessments is to identify critical entities and assist the implementation of resilience measures. The assessments shall be carried out whenever necessary, and at least every four years.[105] In Member State risk assessments, a broad range of risks must be considered, including natural and man-made risks, accidents, natural disasters and hybrid or other antagonistic threats and cross-border and cross-sectoral risks. The assessment shall further account

---

egy and its Action Plan: An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats' JOIN (2023) 8 final, 4 and 9-12.

[102] Becker (n 101) 1.

[103] CER Directive Article 6(1).

[104] CER Directive Article 1(a-b); see also Article 2(5) defining 'essential service'.

[105] CER Directive Article 5(1); see also CER Article 6 and 13; the first Member State risk assessment was to be executed by 17 January 2026.

for risks arising from the interdependence between sectors, including their dependence on entities located in other Member States and third countries and the potential impact that significant disruptions in one sector may have on others. Member States shall share relevant elements of their risk assessments with identified critical entities and cooperate with other Member States as well as, where appropriate, third countries in addressing cross-border risks.[106]

Based on these assessments, Member States shall identify critical entities. In order to qualify as critical, the entity shall provide at least one essential service and operate in the territory of the Member State identifying it as critical and further, a disruption of it shall entail significant disruptive effects on the essential services it provides, or on other essential services that depend on them.[107] To assess whether a disruptive effect is significant or not, aspects such as scale, duration and economic, societal and environmental impacts as well as the geographical scope, including cross-border impacts, are considered.[108] The Directive additionally recognises critical entities of particular European significance, meaning critical entities which provide essential services to or in six or more Member States. Such entities are subject to additional coordination and advisory mechanisms involving the Commission and affected Member States.[109]

Member States shall, according to CER Article 10, furthermore support critical entities in the enhancement of their resilience, through *inter alia* guidance, resilience exercises and training of personnel. Where necessary and justified, Member States may also provide financial support to critical entities. The Directive also emphasises cooperation and information exchange between Member States, competent authorities and critical entities, particularly in regard to cross-border infrastructure and entities operating across multiple Member States. The cooperation aims to ensure consistent application of the Directive across the Union. The Directive has further established a Critical Entities Resilience Group aimed at facilitating cooperation, information sharing and the exchange of best practices between Member States and the Commission, in relation to cross-border risks and incidents.[110]

Supervision and enforcement provisions are established in Article 21 which enables authorities to, for example, conduct on-site inspections and audits, request relevant information from critical entities, as well as order corrective measures where necessary. Article 22 further requires Member States to provide for effective, proportionate and dissuasive penalties for infringements of national measures implementing the Directive.

[106] CER Article 5(1)-(3).
[107] CER Article 6(1)-(2).
[108] CER Article 7(1).
[109] CER Article 17-18.
[110] CER Articles 9(2), 11 and 19.

4.1.3 Risk Management, Resilience Measures and Incident Response

Reflecting several aspects of the national risk assessments conducted by Member States, critical entities shall also conduct entity-specific risk assessments pursuant to Article 12. The purpose of these assessments is to identify all relevant risks capable of disrupting the provision of essential services. The assessments shall be based on all relevant information and shall also consider the interdependencies between sectors, including both the extent to which other sectors depend on the services provided by the critical entity and the extent to which the critical entity depends on essential services provided by other entities, including in other Member States and in third countries.

Furthermore, the Directive requires Member States to ensure that critical entities implement appropriate and proportionate technical, security and organisational measures. These measures shall be based on the risk assessments of both the Member State and the critical entity, with the purpose of preventing incidents and ensuring the adequate physical protection of their premises and critical infrastructure. Such measures may include personnel security measures for example, background checks in duly reasoned cases for individuals holding sensitive roles relating to the resilience of critical entities.[111]

In the event of an incident, critical entities are also required to take measures necessary to respond to, resist and mitigate its consequences as well as to guarantee recovery and the continuity of the provision of essential services.[112] CER Article 15 also establishes obligations for critical entities to, without undue delay after becoming aware of an incident, notify the competent authorities of incidents that significantly disrupt, or have the potential to significantly disrupt, the provision of essential services. Where incidents have, or may have, significant cross-border effects affecting six or more Member States, the Directive further provides for notification to the Commission and information sharing between affected Member States.

4.2 The NIS2 Directive

Contemporary threats against subsea infrastructure are not limited to physical interference and sabotage. The operation, monitoring and management of submarine cables, pipelines and related maritime infrastructure increasingly rely on interconnected digital and communication system for remote control, communication and logistics, making such infrastructure highly vulnerable to cyberattacks capable of disrupting their operation and security.[113] The NIS2 Directive forms an important complement to the EU resili-

[111] CER Articles 13(1) and 14(1).
[112] CER Article 13(1).
[113] Liebetrau and Bueger (2022) (n 3) 1-2.

ence framework by strengthening cybersecurity and risk management obligations relating to critical infrastructure and essential entities within the Union.

The connection between the CER Directive and the NIS2 Directive is emphasised in the preamble to both directives. It is established that the CER Directive and its provisions on physical security of critical entities are to be understood in conjunction with the NIS2 Directive and its cybersecurity dimension of critical infrastructure protection. Physical and cybersecurity risks are viewed as interdependent and are thus jointly managed through the two directives. Consequently, entities identified as critical under CER are to be considered essential under NIS2, reflecting the difference in terminology in the two directives.[114]

The implementation of NIS2 also follows the criticism earlier cybersecurity regulation faced. The original NIS Directive[115] was criticised for having an insufficient scope and for producing fragmented implementation across Member States, especially in regard to the identification of operators of essential services and incident-reporting thresholds.[116] NIS2 addresses these shortcomings by strengthening harmonisation across the Union through broader sectoral coverage, more uniform reporting and notification requirements, stricter enforcement mechanisms and measures for consistency with other regulatory frameworks.[117]

4.2.1 Scope and Key Concepts

Article 1 of NIS2 describes the aim of the Directive as achieving a high uniform level of cybersecurity across the Union as a means to improve the functioning of the internal market. To this end, NIS2 establishes obligations for Member States to adopt national cybersecurity strategies, such as designating particular cyber crisis management authorities. Additionally, NIS2 lays down obligations regarding the Member State supervision, enforcement and cybersecurity information sharing.

The Directive primarily applies to entities of a certain size, operating in sectors of high criticality, as set out in its Annexes. These sectors include, inter alia, energy and digital infrastructure, covering entities that provide services such as electricity, oil and gas, as well as essential internet infrastructure,

[114] NIS2, preamble (30) and Article 3(1)(f); CER, preamble (9).

[115] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

[116] Agnieszka Besiekierska 'Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive' in Dragan Čišić and others (eds), 2023 46th ICT and Electronics Convention (MIPRO): Proceedings (Croatian Society for Information, Communication and Electronic Technology 2023) 1474, 1475.

[117] Alexopoulos, Niemi, Skobiej and Sill Torres (n 5) 667, 669.

connectivity and digital services.[118] In addition, the Directive extends its scope to certain entities regardless of their size where their services are of particular importance for critical societal or economic activities or where disruptions could have significant cross-border or systemic effects. Most notably however, entities identified as critical entities under the CER Directive automatically fall within the scope of NIS2, further highlighting the close connection between the two Directives.[119] While the Directive distinguishes between essential and important entities, the infrastructure at hand falls within the category of essential entities, as previously noted, due to its identification as critical under the CER Directive.[120]

Cybersecurity refers to activities necessary to protect network and information systems, their users and other persons affected by cyber threats.[121] Cyber threats are understood as potential circumstances, events or actions capable of adversely affecting network and information systems, their users or other persons.[122]

The Directive additionally establishes jurisdictional rules in Article 26 determining which Member State exercises supervisory competence over entities falling within its scope. As a general rule, entities fall under the jurisdiction of the Member State in which they are established, with an exception for certain digital infrastructure and service providers with cross-border operations.

4.2.2 Risk Management and Cybersecurity Obligations

A central element of the NIS2 Directive is the requirement for entities to adopt appropriate and proportionate cybersecurity risk management measures. Article 21 provides that essential entities shall take technical, operational and organisational measures to manage risks posed to the security of network and information systems. These measures are aimed at preventing and minimising the impact of incidents and ensuring the continuity of essential services. They include, inter alia, risk analysis, incident handling, business continuity, supply chain security as well as cybersecurity training for actors in contact with the entities and general human resources security. In this regard, entities are required to take account of vulnerabilities specific to their direct suppliers and service providers, as well as the overall quality of their cybersecurity practices. They must also consider the results of coordinated security risk assessments of critical supply chains carried out at Union level. Entities who fail to comply with these requirements are further-

[118] NIS2, Article 2(1) and Annex I, points 1 and 8.

[119] NIS2, Article 2(2)-2(3).

[120] NIS2, Article 3(1)(f); see also NIS2 preamble (30).

[121] NIS2, Article 6(3), referring to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act) [2019] OJ L151/15, Article 2(1).

[122] NIS2, Article 6(10), referring to Cybersecurity Act (n 124) Article 2(8).

more required to take all necessary, appropriate and proportionate corrective measures, without undue delay.[123]

In addition to preventive measures, the Directive establishes obligations relating to incident reporting. Through Article 23, entities are required to notify competent authorities of significant incidents without undue delay, thus enabling coordinated responses and information sharing at both national and Union level.

4.2.3 Supervision, Enforcement and Cooperation

The NIS2 Directive further establishes a framework for supervision, enforcement and cooperation between Member States. Member States are required to designate or establish competent authorities responsible for cybersecurity supervision and oversight of the implementation of the Directive.[124] Article 31 further provides that Member States are required to ensure that competent authorities effectively supervise and take necessary action to ensure compliance with the Directive. The Directive distinguishes between supervisory regimes for essential and important entities, with stricter supervision applying to essential entities. In relation to essential entities, competent authorities are empowered to exercise both *ex ante* supervisory measures, including inspections, audits and requests for information, as well as *ex post* enforcement powers, such as binding orders for corrective measures where necessary.[125]

The Directive establishes enforcement mechanisms and sanctioning regimes in relation to infringements of cybersecurity obligations. Member States are required to provide for effective, proportionate and dissuasive penalties, while significant administrative fines may be imposed for infringements of obligations concerning cybersecurity risk-management measures and reporting obligations.[126]

NIS2 also contains provisions relating to cybersecurity information sharing, voluntary notifications and cooperation between entities, competent authorities and cybersecurity incident response teams concerning cyber threats, incidents and near misses.[127] For entities operating or providing services in more than one Member State in particular, Article 37 establishes cross-border cooperation and mutual assistance between Member States in relation to supervisory and enforcement activities.

[123] NIS2, Article 21(3) and (4).
[124] NIS2, Article 8.
[125] NIS2, Article 32 and recital 122, see also Article 33.
[126] NIS2, Articles 34(4)-(5), read together with Articles 21 and 23, and 36.
[127] NIS2, Articles 29-30.

4.3 EU Action Plan on Cable Security

As a complementary policy instrument the EU Action Plan on Cable Security builds upon the broader resilience framework established by the CER and NIS2 Directives. In response to the increasing threats against subsea infrastructure, particularly in the Baltic Sea, the Commission sets out a coordinated and holistic approach addressing the full resilience cycle of subsea infrastructure through four priorities: prevention, detection, response and repair, and deterrence. The Action Plan emphasises EU-level coordination, information sharing and cooperation between Member States throughout all of the stages in the resilience cycle. Although Member States remain primarily responsible for infrastructure protection, the Action Plan argues that EU-level support for the most impacted States is necessary to ensure security across the Union due to the cross-border nature and economic importance of submarine cables. While primarily focused on submarine cables, the measures outlined may be extended to other forms of critical maritime infrastructure, such as pipelines.[128]

4.3.1 Prevention

In relation to prevention, the Action Plan emphasises the importance of effectively implementing existing EU legal frameworks, in particular the CER and NIS2 Directives. Member States are encouraged to strengthen the identification of critical entities and to ensure the adoption of appropriate resilience and cybersecurity measures. Additionally, the Action Plan further promotes the mapping of existing and planned submarine cable infrastructure as well as the establishment of an EU-level framework for strategic cable projects, aimed at increasing resilience.[129]

4.3.2 Detection

With regard to detection, monitoring and surveillance of subsea infrastructure are identified as key elements of resilience. The Plan proposes improved situational awareness and enhanced monitoring in order to facilitate the early detection of incidents affecting subsea infrastructure.[130]

4.3.3 Response and repair

In its approach to response and repair, the Action Plan emphasises the need for improved coordination between existing EU crisis management frameworks. A key operational challenge relating to the repair of damaged cables identified in the Action Plan is the limited availability of vessels with specialised repair capabilities. In the case of simultaneous and systemic attacks to cables across the Union, the current capacity of such vessels to intervene

[128] EU Action Plan, 2 and 17.
[129] EU Action Plan, 3-6.
[130] EU Action Plan, 9-11.

and repair in time is insufficient. Therefore, the Action Plan proposes the development of coordinated repair mechanisms.[131]

4.3.4 Deterrence

The Action Plan's deterrence dimension focuses on strengthening the Union's ability to prevent and respond to hostile acts targeting subsea infrastructure and hold perpetrators accountable. The Action Plan highlights the use of existing EU instruments, including sanctions regimes and broader frameworks addressing hybrid threats, while also emphasising the importance of improving attribution and countering strategies used for plausible deniability in hybrid operations.[132] Particular attention is given to so-called "shadow fleets" often associated with cable damage and the circumvention of sanctions. The Action Plan further emphasises cooperation with flag and port States to enhance accountability for vessels suspected of harmful activities. It further highlights the relevance of existing legal frameworks under UNCLOS when assessing measures against vessels operating on the high seas.[133]

4.4 Strengths and challenges of the EU resilience framework

The interdependence between physical and cybersecurity aspects of critical infrastructure protection is established through both the CER and the NIS2 Directives and is the reason the two directives are designed to operate alongside one another.[134] Consequently, many of the broader structural strengths and weaknesses identified in relation to one of the Directives, may similarly be relevant to the other.

The EU resilience framework established through these Directives has attempted to address the weaknesses identified in the implementation of their predecessors, which left considerable discretion left to Member States resulting in diverging national approaches and fragmented legal regimes for operators across the Union. In comparison, NIS2 has established broader sectoral coverage and more extensive cybersecurity obligations relating to risk management, incident reporting and supply-chain security. The coordinated risk assessments of critical supply-chains at Union level particularly shows how the increasingly interconnected and cross-border nature of cybersecurity risks affecting critical infrastructure are considered. NIS2 also strengthens supervision and enforcement through significant administrative fines which increases managerial responsibility for compliance with cybersecurity obligations. Directors and managers may therefore be held accountable for failures to comply with cybersecurity risk-management obligations,

[131] EU Action Plan, 13–15.
[132] EU Action Plan, 14-15.
[133] EU Action Plan, 17.
[134] CER, recital 9; NIS2, recital 30.

while competent authorities may impose corrective measures where entities fail to fulfil their obligations.

However, potential challenges concerning the practical implementation of the broader EU resilience framework have been identified. In relation to CER specifically, it has been noted that the Directive leaves considerable interpretative flexibility to Member States regarding the identification of critical entities and resilience measures, as well as lacking a standardised framework for assessing resilience across the Union. The insufficient specificity in CER may reduce its effectiveness in practice.[135] Similar concerns have been raised regarding the new cybersecurity framework.[136] While the Directive is binding as EU law, it still leaves considerable discretion to national authorities regarding its implementation. The effectiveness of the framework may therefore, similarly to its predecessor, be undermined by weak or uneven implementation causing fragmentation across Member States. The progress of NIS2's implementation so far varies widely across the Union, thus leaving the question of its effectiveness through the perspective of a harmonised national implementation across the Member States, unclear.[137]

The main governance challenge behind critical maritime infrastructure protection is the transnational and interconnected nature of maritime infrastructure, together with complex ownership structures and the involvement of multiple policy sectors, authorities and private actors. Effective protection and resilience are therefore dependent on coordination between industry and governments, as well as between States and regional institutions.[138]

In this regard, the EU Action Plan on Cable Security illustrates the increasing emphasis placed on coordinated approaches to subsea infrastructure protection within the broader EU resilience framework. Although the Action Plan does not constitute binding legislation, it complements the two Directives by outlining strategic priorities and practical measures concerning the protection of submarine cables.

In the literature it has been emphasised that the increasing density and interconnectivity of maritime infrastructure necessitates frameworks that can operate across sectors and jurisdictions, including territorial seas, EEZs and the high seas. Legal harmonisation, trusted information-sharing and regional multistakeholder cooperation have been identified as central elements of effective critical maritime infrastructure protection and are notably such

[135] Alexopoulos, Niemi, Skobiej and Sill Torres (n 5), 667-668.

[136] Besiekierska (n 118), 1475-1476.

[137] Theodoros Karathanasis, *Cybersecurity and EU Law: Adopting the Network and Information Security Directive* (Routledge 2024) 237-239.

[138] Tobias Liebetrau and Christian Bueger, 'Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity' (2024) 46 International Journal of Critical Infrastructure Protection 100683, 2.

qualities found in the EU's cybersecurity and maritime security initiatives, including NIS2.[139]

While the provisions of the EU resilience frameworks have been used as a positive example of effective critical maritime infrastructure protection, warnings have still been raised due to the potential risks of fragmentation within the EU regime. A reason for this concern is the involvement of multiple EU institutions, agencies and national authorities in the framework, as well as differing national organisational structures and implementation approaches. Effective horizontal and vertical coordination between these actors has therefore been highlighted as essential for ensuring coherent governance and resilience across the Union, as well as a synchronisation of EU efforts with the initiatives of external partners such as NATO.[140]

The CER Directive differs significantly from its predecessor, with a broader scope and ambition and mainly targeting resilience instead of protection. However, some of the core features of the CER Directive are evolved versions of the provisions in the ECI Directive, making it unclear if the changes of the new CER Directive are enough to adequately address the weaknesses earlier frameworks had for critical infrastructure protection.[141] While the new EU resilience framework share certain characteristics with its predecessors that raises concerns regarding the effectiveness of its practical effect, the Directives are still in an early stage of implementation. Thus, despite these potential issues the Directives at least drive the enhancement of critical maritime infrastructure resilience forward.[142]

Taken together, the CER and NIS2 Directives establish a detailed and coordinated regulatory framework for the physical and cybersecurity resilience of critical subsea infrastructure within the EU. Although the EU Action Plan does not constitute binding legislation, it illustrates the EU's increasing focus on subsea infrastructure protection against the contemporary threats in the Baltic Sea region. Due to the nature of EU law, through its institutional enforcement mechanisms and CJEU's compulsory jurisdiction, the CER and NIS2 Directives have a more direct influence on the governance of subsea infrastructure within the EU than traditional international law frameworks such as UNCLOS. This is especially relevant in the Baltic Sea region, where nearly all coastal States are members of the EU.[143]

[139] Liebetrau and Bueger (2024) (n 140), 2 and 4.

[140] Liebetrau and Bueger (2024) (n 140), 6; Alexopoulos, Niemi, Skobiej and Sill Torres (n 5) 672.

[141] Becker (n 101), 2.

[142] Alexopoulos, Niemi, Skobiej and Sill Torres (n 5) 673.

[143] On the institutional characteristics of EU law in maritime governance, see Langlet (n 98) 281.

5 Analytical Discussion

The aim of this thesis has been to examine the extent to which the CER and NIS2 Directives complement the UNCLOS regime's governance of submarine cables and pipelines in relation to contemporary threats in the Baltic Sea. For this purpose, this concluding analysis synthesises the findings of the previous chapters and addresses the thesis' research questions in light of the broader relationship between the UNCLOS regime and the EU resilience framework.

What legal framework does UNCLOS establish for submarine cables and pipelines and what structural limitations does it present for their protection?

While UNCLOS is the central international instrument governing the law of the sea, it functions primarily as an umbrella framework. Thus, its main function is not maritime infrastructure protection, which naturally creates limitations in relation to the effective protection of submarine cables and pipelines. It is, nevertheless, a foundational legal instrument and reflects customary international law in relation to the EEZ, continental shelf and the high seas. As all Baltic Sea States, alongside the EU, are Parties to the Convention, UNCLOS has a further significance in the Baltic Sea context.

Within its territorial sea, the coastal State exercises sovereignty over the waters, seabed and subsoil in a manner comparable to its sovereignty over land territory. Although foreign vessels enjoy the right of innocent passage, such passage must not be prejudicial to the peace, good order or security of the coastal State. Within the territorial seas, coastal States retain comparatively strong regulatory and enforcement powers. Consequently, submarine cables and pipelines located within territorial waters are relatively protected from interference from vessels navigating the area compared to infrastructure located in other maritime zones. Navigation conducted with the purpose of damaging or interfering with infrastructure would not qualify as in innocent passage, allowing the coastal State to prevent such passage and to intervene against malicious activities.

The legal framework changes considerably beyond territorial waters. Within the EEZ, the coastal State exercises limited sovereign rights rather than full sovereignty, while other States retain the important high seas freedoms of navigation and the laying and maintaining of submarine cables and pipelines. Through the due regard obligation, UNCLOS seeks to balance these competing rights and interests.

In the Baltic Sea context, the continental shelf largely overlaps geographically with the seabed beneath the EEZ, meaning that the governance of subsea infrastructure often involves the simultaneous application of the legal regimes relating to both maritime zones. Although coastal States retain cer-

tain rights relating to resource exploitation and pipeline routing, the laying and maintenance of subsea infrastructure on the continental shelf remains subject to significant freedoms enjoyed by other States. Coastal State rights must therefore coexist with the rights and freedoms of other States under UNCLOS.

Through this, the UNCLOS framework facilitates international navigation and the transnational development of maritime infrastructure. At the same time however, this structure also creates limitations regarding the protection of subsea infrastructure. Governance of submarine cables and pipelines beyond the territorial sea is not based on exclusive coastal State control and UNCLOS does not establish a system of universal jurisdiction in relation to incidents affecting subsea infrastructure. Instead, enforcement beyond territorial seas primarily relies on flag State jurisdiction and inter-State cooperation between the flag State and the affected State. In practice, this may limit effective enforcement, as the State possessing jurisdiction over a given incident may not always have an interest in pursuing enforcement action. There might particularly be a lack of political willingness for such enforcement action where incidents involve foreign-flagged vessels or the damage is an act of state sponsored sabotage.

The transnational nature of submarine cables and pipelines further complicates their protection under UNCLOS. Because subsea infrastructure often extends across multiple maritime zones, its governance does not always align with UNCLOS's zonal and jurisdiction-based structure which creates difficulties for effective protection in incidents involving cross-border subsea infrastructure, particularly where enforcement powers remain divided between multiple States and maritime zones. While coastal States possess comparatively strong enforcement powers within their territorial waters, these powers become significantly more limited in the EEZ and on the continental shelf, leaving cables and pipelines vulnerable to interference. Actors seeking to damage subsea infrastructure may instead operate in maritime zones where coastal State enforcement powers are more limited and can thus avoid the inconvenience of adhering to the rules of innocent passage. The powers and protective measures available for coastal States to secure subsea infrastructure are hence not enough to protect cables and pipelines in maritime zones beyond the territorial sea.

These structural limitations are closely connected to the broader purpose and design of the Convention. The UNCLOS regime was primarily developed to regulate competing maritime rights and freedoms rather than contemporary hybrid threats directed against critical infrastructure. Consequently, recent incidents in the Baltic Sea expose how the Convention's traditional jurisdictional structure may struggle to address modern security challenges affecting subsea infrastructure.

That being said, UNCLOS does not leave subsea infrastructure entirely unprotected. The Convention requires States to criminalise the breaking or injury of submarine cables and pipelines by ships flying their flag or persons subject to their jurisdiction. It further provides that persons causing damage to existing infrastructure during the laying or repair of other infrastructure shall bear the costs of repair and establishes a compensation mechanism where fishing gear has been sacrificed in order to avoid damaging submarine cables or pipelines. These provisions demonstrate that the Convention recognises the protection of subsea infrastructure as an important legal interest, even if its broader jurisdictional structure limits the practical enforcement powers available for such protection. Read together with the Convention's purpose, UNCLOS cannot reasonably be interpreted as permitting deliberate damage to subsea infrastructure in disregard of the interests of States seeking to preserve such infrastructure intact.

Prompted by the recent threats against subsea infrastructure in the Baltic Sea and by the apparent structural limitations of UNCLOS, it has been argued that a rigid flag State-centred understanding of jurisdiction beyond territorial seas does not reflect the broader object and purpose of UNCLOS. As the Convention is based on principles such as good faith, State cooperation, peaceful use of the sea and due regard for the rights and interests of other States, UNCLOS cannot reasonably be interpreted as protecting actors engaging in sabotage under the freedom of navigation or as preventing the investigation of vessels reasonably suspected of involvement in such conduct. Certain ITLOS and arbitral decisions can be interpreted as supporting such a view as they have indicated a willingness to accept broader coastal State measures within the EEZ, even where such powers are not expressly provided.

While this thesis supports a more dynamic interpretation of UNCLOS in relation to contemporary threats in the Baltic Sea, the practical significance of such interpretations remains uncertain until they are further clarified or confirmed through international judicial or arbitral practice. UNCLOS therefore continues to provide limited mechanisms for the protection of subsea infrastructure beyond territorial seas. These structural characteristics therefore explain the increasing importance of complementary resilience-oriented frameworks within the EU.

How do the CER and NIS2 Directives regulate the governance, resilience and protection of critical subsea infrastructure within the EU?

In contrast to UNCLOS, the CER and NIS2 Directives establish a more operational and coordinated resilience framework for the protection of critical subsea infrastructure within the EU. Rather than primarily regulating competing maritime rights and freedoms, the Directives seek to strengthen resil-

ience of and manage vulnerabilities affecting critical infrastructure and essential services.

Rather than treating critical infrastructure protection solely as a national security issue, the CER Directive introduces a broader framework focused on resilience, risk management and coordination. Through obligations relating to national and entity-specific risk assessments, cross-border cooperation and incident reporting, the Directive seeks to address disruptions affecting cables and pipelines that may produce adverse effects across multiple sectors and Member States. Particularly important is the Directive's emphasis on interdependencies between sectors and Member States as it indicates an awareness that such disruptions may produce cascading effects extending beyond the State in which the incident occurs. Consequently, the framework promotes a more coordinated approach to infrastructure protection within the Union.

The CER Directive further illustrates the increasing role of EU institutions in areas traditionally dominated by national competence. While Member States remain primarily responsible for identifying critical entities and implementing resilience measures, the Directive introduces obligations concerning cooperation, information sharing and supervision at Union level. This reflects an increasing recognition that the protection of critical infrastructure cannot be addressed solely through domestic frameworks.

NIS2 complements the framework by extending resilience to also include the cybersecurity dimension of subsea infrastructure protection. The Directive reflects the increasing dependence of submarine cables, pipelines and related maritime infrastructure on interconnected digital systems and therefore approaches physical and cybersecurity threats as closely interconnected.

NIS2 additionally strengthens the operational dimension of resilience governance through its more extensive supervisory and enforcement mechanisms. Through obligations relating to cybersecurity risk-management, incident reporting, supply-chain security and business continuity, the Directive attempts to reduce vulnerabilities before incidents occur rather than primarily regulating responsibility after damage has already taken place. The Directive therefore reflects a more preventative and resilience-oriented approach.

Another important aspect of the EU resilience framework is its attempt to reduce fragmented approaches to critical infrastructure protection between Member States. The CER and NIS2 Directives introduce obligations concerning cooperation, supervision and information sharing aimed at promoting more coherent implementation across the Union. This is particularly

relevant in relation to cables and pipelines as they often extend across several sectors and jurisdictions.

Nevertheless, the effectiveness of the resilience framework remains dependent on implementation by Member States and coordination between national authorities, EU institutions and private actors. Both CER and NIS2 leave considerable discretion to Member States regarding implementation, supervision and organisational structures, which may result in uneven application across the Union. Such inconsistencies may be especially problematic in relation to cables and pipelines due to them frequently extending across several jurisdictions, which require coherent and uniform implementation as well as effective cross-border cooperation between Member States.

The EU Action Plan on Cable Security further demonstrates how subsea infrastructure protection is increasingly approached within the EU as a broader resilience and security issue rather than solely traditional infrastructure protection. Although the Action Plan does not constitute binding legislation, it complements CER and NIS2 by identifying strategic priorities relating to prevention, detection, response and deterrence. Particularly significant is the Action Plan's emphasis on coordinated repair capabilities, monitoring, information sharing and the attribution difficulties associated with hybrid threats and plausible deniability.

Taken together, the CER and NIS2 Directives establish a broader resilience-oriented framework aimed at strengthening the physical and cybersecurity protection of critical subsea infrastructure within the EU. The Directives reflect the EU's effort to address contemporary threats affecting subsea infrastructure in the Baltic Sea region.

To what extent do CER and NIS2 complement the UNCLOS regime in strengthening the governance, resilience and protection of critical subsea infrastructure?

Having examined the legal frameworks established by UNCLOS and the CER and NIS2 Directives separately, the following discussion considers their broader relationship in the Baltic Sea context.

From the previous analysis, it becomes clear that UNCLOS and the EU resilience Directives approach subsea infrastructure from fundamentally different perspectives. While UNCLOS primarily governs the allocation of rights and jurisdiction between States in different maritime zones, CER and NIS2 focus more directly on the protection and continuity of critical infrastructure within the EU. In this respect, the Directives do not replace the UNCLOS regime but rather supplement certain structural limitations relating to the protection of subsea infrastructure against contemporary threats in the Baltic Sea.

A central limitation of UNCLOS is that the protection of infrastructure beyond the territorial sea largely depends on flag State jurisdiction, due regard obligations and cooperation between States. As demonstrated by recent incidents in the Baltic Sea, such a structure may complicate effective enforcement and coordinated responses where incidents involve foreign-flagged vessels, multiple jurisdictions or suspected hybrid threats. The EU instruments attempt to address some of these issues through more detailed practical obligations concerning risk assessments, information sharing, supervision and cross-border cooperation. In contrast to UNCLOS's primarily jurisdiction-based structure, CER and NIS2 introduce a more operational approach aimed at reducing vulnerabilities before disruptions occur as well as incident response in the event of such a disruption.

The relationship between CER and NIS2 further illustrates this supplementary function. The Directives are closely connected through both their preambles and substantive provisions, which seek to align physical and cybersecurity measures relating to critical infrastructure. This contributes to a more integrated approach to the protection of subsea infrastructure and reduces the risk of fragmented responsibilities between authorities and sectors. At the same time, the extent to which the EU framework can address the structural limitations of UNCLOS should not be overstated. Although CER and NIS2 introduce more detailed obligations and coordination mechanisms, implementation ultimately remains dependent on Member States. The Directives therefore cannot fully eliminate fragmentation or jurisdictional complexity, particularly where subsea infrastructure extends across several jurisdictions or maritime zones.

Additional difficulties may arise as CER and NIS2 are primarily implemented at a national level. While Member States remain responsible for identifying critical entities and implementing protective measures within their jurisdictions, submarine cables and pipelines frequently extend across several maritime zones and may simultaneously affect multiple States. The Directives therefore do not fully resolve the practical and jurisdictional difficulties that arise where interconnected infrastructure is shared between different jurisdictions. Such difficulties may become particularly significant in relation to infrastructure located within the EEZ and on the continental shelf, where UNCLOS continues to govern the allocation of rights and jurisdiction between States

Due to the relationship between the EU and UNCLOS, the EU resilience framework continues to operate within the broader jurisdictional structure established by the Convention. As both the EU and all Baltic Sea Member States are Parties to UNCLOS, CER and NIS2 cannot eliminate the jurisdictional limitations established under the Convention in maritime zones beyond the territorial sea. Many submarine cables and pipelines in the Baltic Sea are located within the EEZ and on the continental shelf, where UN-

CLOS continues to govern the allocation of rights and jurisdiction between States. The Directives may therefore strengthen resilience, incident response and coordination within the EU, but they cannot fully resolve the jurisdictional complexities that arise where subsea infrastructure extends across several maritime zones and national jurisdictions.

Nevertheless, the EU framework appears particularly significant in the Baltic Sea context due to the high degree of regional integration between the surrounding coastal States. Compared to traditional international law instruments, CER and NIS2 have a more direct impact on national legal systems through the primacy of EU law and the supervisory and enforcement functions exercised by the European Commission and the CJEU. In this respect, the Directives introduce a greater degree of harmonisation and institutional coordination than what follows from UNCLOS alone. The EU Action Plan further contributes to this aim by identifying concrete priorities and measures relating to address the threats affecting submarine cables.

Taken together, the CER and NIS2 Directives complement the UNCLOS regime by addressing several governance and resilience-related challenges that UNCLOS was not originally designed to manage. While UNCLOS continues to provide the foundational legal framework governing subsea infrastructure in maritime zones beyond the territorial sea, the EU resilience framework introduces more detailed mechanisms aimed at strengthening the governance and protection of submarine cables and pipelines in the Baltic Sea region.

6 Conclusion

The purpose of this thesis has been to examine the extent to which the EU resilience framework, particularly the CER and NIS2 Directives, complements the UNCLOS regime's governance of submarine cables and pipelines in relation to contemporary threats in the Baltic Sea. The analysis demonstrates that UNCLOS and the EU resilience framework approach the protection of subsea infrastructure from fundamentally different perspectives and fulfil partly different functions within the broader governance of subsea infrastructure.

The thesis has shown that UNCLOS provides the foundational legal framework governing submarine cables and pipelines in maritime zones beyond the territorial sea. Through the allocation of rights and jurisdiction between States, the Convention facilitates international navigation and the transnational development of subsea infrastructure. At the same time, the analysis demonstrates that the UNCLOS regime presents structural limitations in relation to the protection of subsea infrastructure against contemporary threats. Beyond the territorial sea, the protection of submarine cables and pipelines largely depends on flag State jurisdiction, inter-State cooperation and due regard obligations rather than exclusive coastal State control. As demonstrated by recent incidents in the Baltic Sea, such a jurisdiction-based structure may complicate effective enforcement where incidents involve foreign-flagged vessels, multiple jurisdictions or suspected hybrid threats. The thesis further argues that while UNCLOS cannot reasonably be interpreted as permitting deliberate damage to subsea infrastructure, the practical scope of coastal State powers beyond territorial seas remains uncertain in several respects.

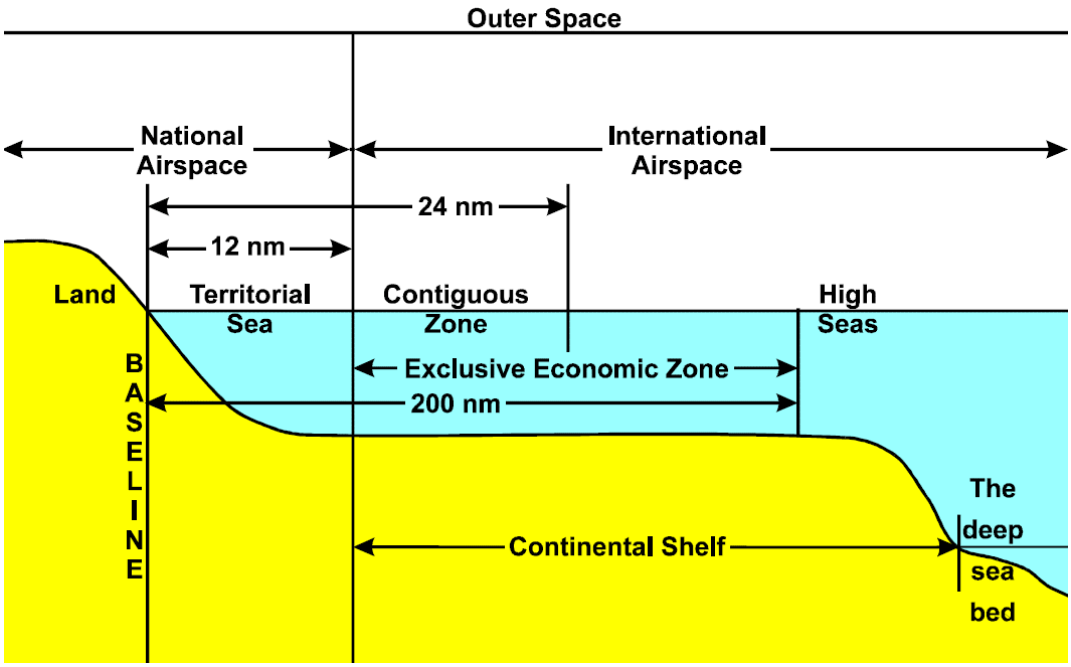
In contrast, the CER and NIS2 Directives establish a more operational framework for the protection of critical infrastructure within the EU. Rather than primarily regulating competing maritime rights and freedoms, the Directives seek to strengthen the continuity and protection of essential infrastructure and services by reducing vulnerabilities and improving the management of disruptions affecting critical infrastructure. The analysis shows that the EU framework places particular emphasis on cross-border cooperation, interdependencies between sectors and Member States, and the interconnected nature of threats affecting subsea infrastructure. NIS2 additionally extends this protection to the cybersecurity dimension of subsea infrastructure, reflecting the increasing dependence of cables, pipelines and related infrastructure on interconnected digital systems.

The thesis nevertheless demonstrates that the extent to which the EU framework can address the structural limitations of UNCLOS should not be overstated. Although CER and NIS2 introduce more detailed obligations and coordination mechanisms, implementation remains dependent on Mem-

ber States and cannot fully eliminate fragmentation or jurisdictional complexity. This is particularly significant in relation to subsea infrastructure, which frequently extends across several maritime zones and jurisdictions. As both the EU and the Baltic Sea Member States remain bound by UNCLOS, the EU resilience framework continues to operate within the broader jurisdictional structure established by the Convention.

Taken together, the analysis demonstrates that CER and NIS2 complement rather than replace the UNCLOS regime. While UNCLOS continues to provide the foundational legal framework governing subsea infrastructure in maritime zones beyond the territorial sea, the EU framework supplements several governance and protection-related limitations that UNCLOS was not originally designed to address. This complementarity appears particularly significant in the Baltic Sea region due to the high degree of regional integration between the surrounding coastal States and the increasing strategic importance of subsea infrastructure for European security, communications and energy supply. The growing focus within the EU on the protection and continuity of critical infrastructure further reflects how subsea infrastructure has increasingly developed from a primarily maritime governance issue into a broader question of regional security and societal stability.

Annex I



Source: MRAG's Website, https://mrag.co.uk/experience/costs-and-benefits-arising-establishment-maritime-zones-mediterranean-sea (accessed 25 May 2026).

Tables of Cases and International Instruments

Cases

North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands) [1969] ICJ Rep 3

Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v Colombia) [2022] ICJ Rep 266

International Instruments

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI

Convention for the Protection of Submarine Telegraph Cables (adopted 14 March 1884, entered into force 1 May 1888) 24 Stat 989; TS 380

Convention on the Protection of the Marine Environment of the Baltic Sea Area (adopted 9 April 1992, entered into force 17 January 2000) 2099 UNTS 197

Convention on the High Seas (adopted 29 April 1958, entered into force 30 September 1963) 450 UNTS 11

International Convention for the Prevention of Pollution from Ships (adopted 2 November 1973, as modified by the Protocol of 1978, entered into force 2 October 1983) 1340 UNTS 184 (MARPOL 73/78)

United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 397

Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331

EU Legislation

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75

Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive) [2008] OJ L 164/19

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L 330/80

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L 333/164

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification [2019] OJ L 151/15

Bibliography

Books and Edited Volumes

Dupuy RJ and Vignes D, 'Submarine Cables and Pipelines' in Rene Jean Dupuy and Daniel Vignes (eds), *A Handbook on the New Law of the Sea*, vol 2 (Brill/Nijhoff 1991) 977

Eckes C, 'European Union Legal Methods – Moving Away from Integration' in Ulla Neergaard and Ruth Nielsen (eds), *European Legal Method – Towards a New European Legal Realism?* (DJØF Publishing 2013)

Franckx E, 'Regulatory Gaps in Baltic Sea Governance' in Henrik Ringbom (ed), *Regulatory Gaps in Baltic Sea Governance: Selected Issues* (Springer International Publishing 2018)

Heintschel von Heinegg W, 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law' in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE Publications 2013) 293

Hettne J and Otken Eriksson I, 'EU-rättsliga tolkningsmetoder' in Jörgen Hettne and Ida Otken Eriksson (eds), *EU-rättslig metod: Teori och genomslag i svensk rättstillämpning* (2nd edn, Norstedts Juridik 2011)

Hjertstedt M, 'Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt' in Ruth Mannelqvist, Staffan Ingmanson and Carin Ulander-Wänman (eds), *Festskrift till Örjan Edström* (Juridiska institutionen, Umeå universitet 2019)

Jareborg N, 'Rättsdogmatik som vetenskap' (2004) *Svensk Juristtidning* 1

Joas M, Ringbom H and Tynkkynen N, 'The Baltic Sea and Global Environmental Change' in Harris PG (ed) *Routledge Handbook of Marine Governance and Global Environmental Change* (Routledge 2022)

Karathanasis T, *Cybersecurity and EU Law: Adopting the Network and Information Security Directive* (Routledge 2024)

Kleineman J, 'Rättsdogmatisk metod' in Maria Nääv and Mauro Zamboni (eds), *Juridisk metodlära* (2nd edn, Studentlitteratur 2018)

Köndgen J and Mörsdorf O, 'The Sources of European Private Law' in Karl Riesenhuber (ed), *European Legal Methodology* (2nd edn, Intersentia 2021)

Reichel J, 'EU-rättslig metod' in Maria Nääv and Mauro Zamboni (eds), *Juridisk metodlära* (2nd edn, Studentlitteratur 2018)

Ringbom H and Lott A, ‘Sabotage of Critical Offshore Infrastructure: A Case Study of the Balticconnector Incident’ in Alexander Lott (ed), *Maritime Security Law in Hybrid Warfare* (Brill 2024) 155

Sandgren C, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation* (4th edn, Norstedts Juridik 2018)

Streinz R, ‘Interpretation and Development of EU Primary Law’ in Karl Riesenhuber (ed), *European Legal Methodology* (2nd edn, Intersentia 2021)

Tanaka Y, *The International Law of the Sea* (4th edn, Cambridge University Press 2023)

Journal Articles

Alexopoulos MJ, Niemi A, Skobiej B and Sill Torres F, ‘Examination of the Critical Infrastructure Resilience Directive from the Maritime Point of View’ (2025) 63(2) *Journal of Common Market Studies* 667

Becker M, ‘Transposing EU-legislation on critical infrastructure protection legal implementation performance in the Baltic Sea region’ (2025) 50 *International Journal of Critical Infrastructure Protection* 100781

Bueger C and Liebetrau T, ‘Critical Maritime Infrastructure Protection: What’s the Trouble?’ (2023) 155 *Marine Policy* 105772

de Witte B, ‘Legal Methods for the Study of EU Institutional Practice’ (2022) 18(4) *European Constitutional Law Review* 637

Hernandez-Benito D, ‘Damages to Submarine Cables and Pipelines in Times of Peace and War: The Nord Stream Sabotage’ (2024) 16(1) *Amsterdam Law Forum* 1

Liebetrau T and Bueger C, ‘Advancing Coordination in Critical Maritime Infrastructure Protection: Lessons from Maritime Piracy and Cybersecurity’ (2024) 46 *International Journal of Critical Infrastructure Protection* 100683

Ringbom H, ’New Threats-Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Subsea infrastructure in the Baltic Sea’ (2025) 56 *Ocean Development & International Law* 390

Conference Proceedings

Besiekierska A, ‘Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive’ in

Dragan Čišić and others (eds), *2023 46th ICT and Electronics Convention (MIPRO): Proceedings* (Croatian Society for Information, Communication and Electronic Technology 2023) 1474

Reference Works

Ehlers P, 'Baltic Sea' in Max Planck Encyclopedia of Public International Law (Oxford University Press online, updated February 2014) https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1252 accessed 16 April 2026

Lagoni R, 'Pipelines' in Max Planck Encyclopedia of Public International Law (Oxford University Press online, updated April 2011) https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e975, accessed 7 May 2026

Policy Documents and Reports

Council of the European Union, *European Union Maritime Security Strategy* (Council of the European Union, 24 June 2014) 11205/14

European Commission, *Action Plan on Cable Security* COM(2024) 150 final

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and its Action Plan: An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats* JOIN (2023) 8 final

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security* JOIN (2025) 9 final

European Commission, Joint Research Centre, 'Submarine cables: how vulnerable are they and can we protect them?' (8 August 2025)

European Policy Centre, 'Battle of the Baltic: Safeguarding Critical Undersea Infrastructure' (22 April 2025)

International Bar Association, *Report of the Task Force on Extraterritorial Jurisdiction* (2008)

International Law Association, 'Third Interim Report of the ILA Committee on Submarine Cables and Pipelines' (2024)

Runde D, Murphy E and Bryja T, *Safeguarding Submarine cables: Protecting Cyber Infrastructure amid Great Power Competition* (Center for Strategic and International Studies, August 2024)

Security Council Report, 'The Nord Stream Incident: Open Briefing' (26 August 2025) https://www.securitycouncilreport.org/whatsinblue/2025/08/the-nord-stream-incident-open-briefing-2.php accessed 24 April 2026

United Nations General Assembly, 'Oceans and the Law of the Sea' (11 December 2023) UN Doc A/RES/78/69

Online Sources

BBC News, 'Why the Strait of Hormuz matters so much in the Iran war' (BBC News, 8 April 2026) https://www.bbc.com/news/articles/c78n6p09pzno accessed 5 May 2026

Ehlers P, 'The Geopolitical History of the Baltic Sea in a New Light' (Swedish Defence University, 27 November 2025) https://www.fhs.se/en/swedish-defence-university/stories/2025-11-27-the-geopolitical-history-of-the-baltic-sea-in-a-new-light.html accessed 19 February 2026

Helsinki Commission (HELCOM), 'Contracting Parties' https://helcom.fi/about-us/contracting-parties/ accessed 20 April 2026

Koshino Y, 'The Changing Submarine Cables Landscape: Expanding the EU's role in the Indo-Pacific' (European Union Institute for Security Studies, Brief, 30 October 2024) https://www.iss.europa.eu/publications/briefs/changing-submarine-cables-landscape accessed 2 March 2026

Lott A, 'The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident' (Lieber Institute for Law and Land Warfare, 26 November 2024) https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/ accessed 25 April 2026

Swedish Ministry of Defence and Ministry of Foreign Affairs, 'Sweden signs Memorandum of Understanding on the protection of critical undersea infrastructure' (21 May 2025) https://www.government.se/press-releases/2025/05/sweden-signs-memorandum-of-understanding-on-the-protection-of-critical-undersea-infrastructure/ accessed 3 May 2025

United Nations Environment Programme, 'Pipeline Blasts Released Record-Shattering Amount of Methane: UNEP study' https://www.unep.org/news-

and-stories/story/pipeline-blasts-released-record-shattering-amount-methane-unep-study accessed 18 April 2026

Åklagarmyndigheten, ‘Åklagaren lägger ned den svenska förundersökningen om grovt sabotage mot Nord Stream’ (7 February 2024) https://www.aklagare.se/for-media/pressmeddelanden/2024/februari/aklagaren-lagger-ned-den-svenska-forundersokningen-om-grovt-sabotage-mot-nord-stream/ accessed 24 April 2026