مجلـــة العلـــوم التربـــوية والدراســـات الإنســـانيـــة
Humanities and Educational Sciences Journal
ISSN: 2709-0302 (online)
ISSN: 2617-5908 (print)

الحماية الدولية للبنية التحتية الرقمية الحيوية: الكابلات تحت سطح البحر والأقمار الصناعية ومراكز البيانات(*)

د/ فارس محمد عبد المحسن الباتع
أستاذ مساعد بكلية الشريعة والقانون
جامعة حائل

*) تاريخ تسليم البحث 15/9/2025 تاريخ قبوله للنشر 21/10/2025
*) موقع المجلة: http://hesj.org/ojs/index.php/hesj/index

الحماية الدولية للبنية التحتية الرقمية الحيوية: الكابلات تحت سطح البحر والأقمار الصناعية ومراكز البيانات

د/ فارس محمد عبد المحسن الباتع
أستاذ مساعد بكلية الشريعة والقانون- جامعة حائل

الملخص

تتناول هذه الدراسة الأمن العالمي للبنية التحتية الرقمية الحيوية، مثل الكابلات البحرية والأقمار الصناعية ومراكز البيانات، باعتبارها أساس الاتصال العالمي والسيادة الرقمية. تستعرض الدراسة الأطر القانونية الحالية، بما في ذلك اتفاقية الأمم المتحدة لقانون البحار، ومعاهدة الفضاء الخارجي، ومبادئ الحوكمة السيبرانية، وتقيّم فعاليتها والفجوات القانونية. باستخدام منهجية نوعية تحليلية، أظهرت النتائج ضعف الحوكمة، ونقص آليات الإنفاذ، وغموض الاستخدام المزدوج، ما يصعب تحميل المسؤولية القانونية. تقترح الدراسة تعزيز القانون الدولي بمسؤوليات جماعية، وإنشاء وكالة عالمية لحماية البنية التحتية الرقمية، وتعزيز الشراكات المحلية في الأمن السيبراني، لضمان المرونة الرقمية والاستقرار والسيادة في عالم مترابط.

الكلمات المفتاحية: البنية التحتية الرقمية، الأمن السيبراني، الكابلات البحرية، الأقمار الصناعية، السيادة الرقمية، القانون الدولي للأمن السيبراني، حوكمة الفضاء السيبراني.

International Protection of Critical Digital Infrastructure: Subsea Cables and Satellites Data Centers

Dr. Fares Mohammed Abdulmohsen Al-Batea
Assistant Professor, College of Sharia and Law, University of Hail

Abstract

This study examines the global security of critical digital infrastructure, including undersea cables, satellites, and data centers, as the foundation of global connectivity and digital sovereignty. It reviews current legal frameworks, including the UN Convention on the Law of the Sea, the Outer Space Treaty, and cyber governance principles, assessing their effectiveness and legal gaps. Using a qualitative analytical methodology, results show fragmented governance, weak enforcement, and dual-use ambiguities, complicating legal accountability. The study recommends strengthening international law with collective protection responsibilities, establishing a Global Digital Infrastructure Protection Agency, and enhancing local cybersecurity partnerships to ensure digital resilience, stability, and sovereignty in an interconnected world.

Keywords: Digital infrastructure, cybersecurity, undersea cables, satellites, digital sovereignty, international cyber law, cyber governance.

المقدمة:

في ظل الثورة الرقمية التي يشهدها العالم، أصبحت البنية التحتية الرقمية الحيوية ركيزة أساسية لاستمرار الحياة الاقتصادية والسياسية والاجتماعية، حيث يعتمد على هذه البنية كل من الاتصالات الدولية، الخدمات المالية، أنظمة الطاقة، والنقل، وحتى القطاعات الحيوية للدفاع والأمن القومي. ومن أبرز هذه البنى التحتية: الكابلات تحت سطح البحر، التي تنقل بيانات الإنترنت بين القارات بسرعة فائقة، والأقمار الصناعية التي توفر الاتصالات والملاحة والمراقبة، ومراكز البيانات التي تخزن وتعالج البيانات الهائلة اللازمة لتشغيل المؤسسات والشركات والحكومات.

ومع توسع الاعتماد العالمي على هذه البنى، تبرز الحاجة الملحة لحمايتها من التهديدات المحتملة، سواء كانت طبيعية كالكوارث البحرية، أو فنية كالأعطال التقنية، أو بشرية كالهجمات السيبرانية أو التخريب المتعمد. وهنا تبرز أهمية الحماية الدولية للبنية التحتية الرقمية الحيوية، باعتبارها ضرورة استراتيجية لضمان استقرار النظام الرقمي العالمي وحماية مصالح الدول والمجتمعات.

أهمية البحث:

تتجلى أهمية هذا البحث في عدة محاور:

1- إلقاء الضوء على البنية التحتية الرقمية الحيوية كعنصر أساسي في الأمن القومي والاقتصادي العالمي.

2- دراسة أطر الحماية الدولية المتاحة لهذه البنى، وتحديد الثغرات القانونية والتنظيمية.

3- تقديم تصور علمي واستراتيجي للتعامل مع التهديدات المتنوعة، بما يعزز التعاون الدولي ويحد من المخاطر السيبرانية والجيوسياسية.

إشكالية البحث:

على الرغم من الأهمية البالغة للبنية التحتية الرقمية الحيوية، إلا أن الحماية الدولية لها تواجه عدة تحديات: تباين القوانين الدولية، غموض المسؤوليات بين الدول والمشغلين الخاصين، والتحديات التقنية المرتبطة بالطبيعة المعقدة للبنى التحتية الرقمية. ومن هنا تنبثق إشكالية البحث: **كيف يمكن تعزيز الحماية الدولية للبنية التحتية الرقمية الحيوية، مثل الكابلات تحت سطح البحر والأقمار الصناعية ومراكز البيانات، في ظل التحديات القانونية والتقنية والسياسية المعاصرة؟**

أسئلة البحث:

ينطلق البحث من مجموعة من التساؤلات الأساسية:

1- ما هي أنواع البنية التحتية الرقمية الحيوية وأهميتها في الاقتصاد والأمن القومي؟

2-ما هي الأطر القانونية الدولية الحالية لحماية هذه البنية؟

3-ما أبرز التهديدات التي تواجه الكابلات البحرية والأقمار الصناعية ومراكز البيانات؟

4-ما الاستراتيجيات والسياسات المقترحة لتعزيز الحماية الدولية للبنية التحتية الرقمية الحيوية؟

أهداف البحث:

يهدف البحث إلى:

1-تحديد البنية التحتية الرقمية الحيوية وأنواعها ووظائفها الأساسية.

2-تحليل الأطر القانونية والتنظيمية الدولية المتعلقة بحمايتها.

3-دراسة التهديدات والتحديات التي تواجه هذه البنية.

4-اقتراح توصيات واستراتيجيات لتعزيز الحماية الدولية وضمان استدامة عملها.

منهج البحث:

اعتمد البحث المنهج الاستقصائي والمنهج الوصفي التحليلي، الذي يجمع بين دراسة النصوص القانونية الدولية، والوثائق التقنية، والتقارير المتخصصة، مع تحليل الدراسات السابقة والممارسات العملية في مجال الحماية الرقمية. كما استخدم البحث المنهج المقارن لدراسة التجارب الدولية المختلفة في حماية الكابلات البحرية، الأقمار الصناعية، ومراكز البيانات، بهدف استخلاص توصيات قابلة للتطبيق.

إن البحث في الحماية الدولية للبنية التحتية الرقمية الحيوية يمثل ضرورة علمية واستراتيجية في عصر تتسارع فيه الأحداث التقنية والجيوسياسية، حيث لا يقتصر التأثير على الدول فحسب، بل يمتد إلى استقرار الاقتصاد العالمي وأمن المجتمعات الرقمية. ومن خلال دراسة هذا الموضوع، يسعى البحث لتقديم رؤية شاملة تجمع بين القانون الدولي، التقنيات الرقمية، والسياسات الاستراتيجية لضمان حماية فعالة ومستدامة لهذه البنى الحيوية.

التمهيد:

في عصر العولمة الرقمية، أصبحت البنية التحتية الرقمية الحيوية محور الحياة الاقتصادية والسياسية والاجتماعية للدول والمجتمعات على حد سواء. فالكابلات البحرية تحت سطح البحر، والأقمار الصناعية، ومراكز البيانات، لم تعد مجرد أدوات تقنية لنقل وتخزين المعلومات، بل صارت أعصاب الاتصال العالمية وركائز السيادة الرقمية للدول، ومفتاحًا لاستمرارية الخدمات الحيوية والاقتصادات الرقمية.

ومع هذا الاعتماد المتزايد، يواجه الأمن العالمي للبنية التحتية الرقمية تحديات متنامية، منها المخاطر التقنية والهجمات السيبرانية، والنزاعات الجيوسياسية، وظهور الاستخدامات المزدوجة للتقنيات، مما يزيد من هشاشة هذه البنى ويهدد استقرار الشبكات الحيوية التي تقوم عليها المجتمعات الحديثة.

ولا يقتصر الاهتمام بحماية هذه البنية على الجانب التقني فحسب، بل يمتد ليشمل الأبعاد القانونية والسياسية والدولية، إذ يمثل الحفاظ على استقرارها وضمان أمنها تحديًا مشتركًا يتطلب تنسيقًا دوليًا ومبادرات استراتيجية متكاملة. فالقدرة على حماية هذه الموارد الحيوية تعني حماية الاقتصاد العالمي، وتعزيز السيادة الرقمية للدول، وضمان استمرار الخدمات الأساسية التي تعتمد عليها الحياة اليومية للملايين حول العالم.

إن إدراك أهمية هذه البنية الحيوية وفهم أبعاد تهديداتها يشكل المدخل الضروري لأي دراسة متعمقة حول الأمن الرقمي الدولي، ويضع الأساس للبحث في السبل القانونية والتقنية والإستراتيجية لحماية هذه الموارد، بما يضمن استدامة الاتصال العالمي واستقرار الشبكات الرقمية في عالم مترابط بشكل متزايد.

المبحث الأول: البنية التحتية الرقمية الحيوية وأمنها الدولي

المطلب الأول: طبيعة البنية التحتية الرقمية، مشكلات القانون الدولي، وأهمية الحماية

يعتمد الاقتصاد المعولم المعاصر بشكل كبير على البنية التحتية الرقمية الحيوية، التي تضم كلاً من المكونات المادية والافتراضية، وتشكل أساس تداول البيانات وتخزينها وضمان توافرها بشكل مستمر. تمثل هذه البنى العمود الفقري للاتصالات العالمية، والمعاملات الاقتصادية، والعمليات العسكرية، حيث تعد الكابلات البحرية، والأقمار الصناعية، ومراكز البيانات تحت سطح البحر من أبرز مكوناتها، وهي مسؤولة عن نقل أكثر من 95% من إجمالي البيانات عالميًا (Bueger and Liebetrau, 2021). تشكل كابلات الألياف الضوئية الرابط الحيوي بين القارات، بينما توفر الأقمار الصناعية الاتصال الفوري، والملاحة، ومراقبة الأرض، وهو ما يجعلها عنصرًا لا غنى عنه في الاقتصاد والدفاع (Ganz et al., 2024). كما يتم تخزين البيانات الرقمية في مراكز البيانات، لتصبح بذلك شرطًا أساسيًا للاقتصاد الرقمي ووظائف الدولة. وتتكامل هذه الأنظمة لتشكيل أطر السيادة الرقمية، بما يعزز قدرة الدولة على التحكم في تدفقات البيانات وضمان أمنها (Ganz et al., 2024).

إن أمن هذه البنية التحتية لم يعد مسألة تقنية بحتة، بل أصبح يمثل قضية أمن دولي وإنفاذ قانون، إذ ساهم الاعتماد العالمي الضعيف على الأنظمة الرقمية العابرة للحدود في زيادة المخاطر التي تتعرض لها هذه الموارد، بما في ذلك تخريب الكابلات تحت سطح البحر، والتشويش على الأقمار الصناعية، والهجمات الإلكترونية على مراكز البيانات (كافانا وآخرون، 2025). ويزيد من تعقيد هذه القضية الترابط بين هذه البنى، مما يجعل مسائل الاختصاص القضائي صعبة، إذ تمتد الأبعاد المادية والسيبرانية للبنى التحتية عبر ولايات قضائية متعددة، بما في ذلك أعالي البحار والفضاء الخارجي. ومن ثم، فإن حماية هذه البنية التحتية ليست مسؤولية دولة واحدة، بل هي ظاهرة عالمية تتطلب وجود أطر تشريعية ومؤسساتية دولية لتنظيمها وضمان سلامتها.

على صعيد القانون الدولي، توجد فجوة كبيرة بين الحاجة إلى حماية البنية التحتية الرقمية الحيوية والقدرة التشريعية القائمة، إذ أن القانون الدولي ما زال مجزأً وغير قادر على مواجهة التحديات الحديثة المرتبطة بالترابط الرقمي والتحديات الهجينة. فقد تم تنظيم حماية الكابلات البحرية بموجب اتفاقية الأمم المتحدة لقانون البحار (UNCLOS)، فيما تنظم معاهدة الفضاء الخارجي (OST) استخدام الأقمار الصناعية، إلا أن هذه الأطر القانونية تم تبنيها في فترة كان فيها الترابط الرقمي محدودًا، ولم تكن التهديدات الهجينة جزءًا من الاعتبارات القانونية آنذاك (Pleasic, 2024). فعلى سبيل المثال، تنص المادتان 79

و113 من اتفاقية الأمم المتحدة لقانون البحار على حماية محدودة للكابلات البحرية، إلا أنها لا تشمل التخريب المتعمد أو الهجمات الإلكترونية (بهات، 2025). وبالمثل، تحظر معاهدة الفضاء الخارجي عسكرة الفضاء، لكنها لا تحدد الإجراءات الواجب اتباعها في حال تعطل الأقمار الصناعية أو تدميرها. هذا النقص في القواعد الملزمة يتيح للجهات الفاعلة استغلال الثغرات، ويضعف القدرة على الرد على الهجمات السيبرانية ومكافحتها (ديميتروف، 2025).

ويكمن الهدف الأساسي لهذا البحث في دراسة أطر الحماية العالمية للبنية التحتية الرقمية الحيوية، بما يشمل الكابلات البحرية، والأقمار الصناعية، ومراكز البيانات، وتقييم مزايا وعيوب الأطر القانونية الحالية، مع تقديم اقتراحات لتعزيز التماسك القانوني وزيادة فاعليتها. ويركز البحث على أسئلة رئيسة تتمثل في كيفية تعزيز القانون الدولي لحماية هذه البنى، وتحديد الثغرات القانونية والمؤسسية في الأطر القائمة، وسبل مواجهة التهديدات الهجينة التي تجمع بين الأبعاد المادية والسيبرانية والمعلوماتية. ويهدف البحث إلى اقتراح نموذج حوكمة متعدد المجالات، يعترف بالترابط بين البنى التحتية البحرية والفضائية والسيبرانية كنظام عالمي متكامل.

تكتسب هذه الدراسة أهميتها من دورها في توسيع المعرفة بمفهوم السيادة الرقمية والأمن الجماعي، إذ أن سلامة الكابلات البحرية لا تمثل مجرد تحد تقني، بل مطلب استراتيجي لاستقرار النظام الدولي (كافانوف وفرانكن وهي، 2025). وقد يؤدي استهداف هذه البنية التحتية إلى شل أنظمة الاتصالات، وتعطيل الأنظمة الاقتصادية، وتعطيل الأنشطة الدفاعية، بينما قد يكون لاستهداف الأقمار الصناعية أو مراكز البيانات تأثير مضاعف على مجالات مختلفة مثل النقل وصناعة الطاقة (Paik, 2025). وعلى المستوى الإقليمي، يستثمر العديد من الدول العربية في التحول الرقمي والبنية التحتية للاتصال، إلا أن بعض هذه الدول تواجه تحديات تتعلق بحوكمة الأمن السيبراني، بما في ذلك ضعف التشريعات الوطنية ونقص التنسيق بين الدول (عبد الرحمن، 2022). وتعد حماية الكابلات البحرية في الخليج العربي والبحر الأحمر ذات أهمية بالغة للأمن الاقتصادي الإقليمي، كونها تشكل ممرًا رقميًا واستراتيجيًا للطاقة (صحيفة العتيبي، 2023).

أما من الناحية النظرية، فتعتمد الدراسة على نظرية البنية التحتية الحيوية، التي تبرز الترابط بين الأنظمة المادية والرقمية كشرط لمرونة الدولة والمجتمع، وتوضح التأثير المحتمل للهجمات الإلكترونية على القطاعات الاقتصادية والعسكرية والإنسانية (ماتسون لارسون، 2023). كما تستند إلى نظرية الحوكمة، التي تؤكد على ضرورة التعاون متعدد الأطراف لإدارة التحديات العابرة للحدود، إذ لا تستطيع دولة واحدة التصدي

لها بمفردها. ومن خلال الجمع بين هاتين النظريتين، يُنظر إلى حماية البنية التحتية الرقمية كجهد دولي مشترك يتطلب تنسيقًا مؤسسيًا وبناء الثقة وابتكارًا قانونيًا متعدد الأطراف.

أما مراجعة الأدبيات فتشير إلى أن الدراسات المتعلقة بأمن البنية التحتية الرقمية شاملة لكنها متقطعة القطاعية. ففي المجال البحري، يرى Guilfoyle et al. (2022) وDimitrov (2025) أن القانون البحري الحالي غير كافٍ لردع أو مقاضاة التخريب المتعمد للكابلات، ويقترح إنشاء أنظمة مراقبة مشتركة وفق اتفاقية الأمم المتحدة لقانون البحار. وفي مجال الحوكمة السيبرانية، يشير Sherman (2021) وNg (2025) إلى أهمية وضع معايير إلكترونية دولية ومعاهدة رقمية عالمية. كما يبرز Ganz et al. (2024) وTréhu and Roberts (2024) أهمية التحكم في تخزين البيانات ونقلها كمحدد للسيادة الوطنية، مما يفتح نقاشات سياسية حول التوطين وحقوق الوصول. وعلى الصعيد الإقليمي، تتناول المصادر العربية أبعاد الحوكمة الرقمية، حيث يناقش الكيلاني (2021) الجوانب القانونية للأقمار الصناعية وقانون الفضاء في الدول العربية، ويربط حمدي (2024) بين التحول الرقمي والأمن القومي في الشرق الأوسط، فيما يضع يوسف (2020) البنية التحتية الحيوية في سياق الأمن الدولي لتعزيز الدبلوماسية الرقمية للمنطقة العربية.

المطلب الثاني: الأطر القانونية الدولية للبنية التحتية الرقمية في البحار والفضاء السيبراني

أولاً: الإطار القانوني في المجال البحري

يعد القطاع البحري أحد المواقع الأساسية للبنية التحتية الرقمية على مستوى العالم، حيث تعتمد نحو 97% من الاتصالات الدولية ونقل البيانات على كابلات الألياف الضوئية تحت سطح البحر (Bueger et al., 2022). وتعتبر اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) الإطار القانوني الأساسي لهذه الكابلات، إذ تنظم بموجب المادتين 79 و113 عملية مدها، وصيانتها، وحمايتها. ومع ذلك، فإن هذه الأحكام تركز أساسًا على حرية التركيب وواجب عدم الإضرار الطوعي، دون توفير آليات إنفاذ ومساءلة متطورة. يؤدي غياب العقوبات المحددة ضد التخريب أو الإهمال إلى وجود ثغرات في الإنفاذ، خصوصًا في المياه الدولية التي تظل فيها مسائل الاختصاص القضائي غير واضحة (العتيبي، 2023). وتشير التقارير الحديثة إلى أن التهديدات الهجينة، التي تجمع بين القرصنة السيبرانية والتدخل المادي، أصبحت تحديًا جديدًا لم يكن متوقعًا عند صياغة اتفاقية الأمم المتحدة لقانون البحار (Bueger et al., 2022). ومن ثم، دعت هذه المستجدات إلى الحاجة لبروتوكولات إضافية أو مبادئ توجيهية تفسيرية لتعزيز حماية الكابلات البحرية ضد زعزعة الاستقرار المتعمد من قبل الجهات الفاعلة الحكومية

وغير الحكومية. ويؤكد الباحثون في المنطقة العربية أن حماية هذه الكابلات أمر جوهري لنجاح السيادة الرقمية والأمن القومي، بالنظر إلى الاعتماد المتزايد على الاتصال الرقمي في المنطقة (عبد الرحمن، 2022). ومن هنا، تبرز الحاجة لتطوير القانون البحري ليشمل آليات إنفاذ جماعي وتحديد أدوار دقيقة للدول الساحلية والمنظمات الدولية.

ثانياً: الإطار القانوني في مجال الفضاء الخارجي

تأسس الإطار القانوني للأنشطة الفضائية على معاهدة الفضاء الخارجي لعام 1967، التي تؤكد على الاستخدام السلمي للأقمار الصناعية، وعدم التملك، وضرورة التعاون الدولي (Blechová, 2025). ومع ذلك، أدت التطورات التكنولوجية الحديثة إلى محدودية المعاهدة في معالجة التحديات القائمة، بما في ذلك تصادم الأقمار الصناعية، والتسلل السيبراني، ووجود أسلحة مضادة للأقمار الصناعية (ASAT). وتشكل هذه التهديدات خطورة على أنظمة الاتصالات الفضائية، كما تمتد آثارها لتشمل البنية التحتية الرقمية العالمية التي تعتمد على الأقمار الصناعية. ويشير غياب لوائح إلزامية لتنظيم استخدام أو اختبار هذه الأسلحة إلى محدودية أدوات القانون الحالي (الكيلاني، 2021). ومن جهة أخرى، يشير الباحثون إلى أن زيادة الاستثمار في مشاريع الأقمار الصناعية الإقليمية، مثل عرب سات ونايل سات، تتطلب مشاركة أكبر للدول العربية في المفاوضات العالمية المتعلقة بأمن الفضاء (حمدي، 2024). وبناءً عليه، يبرز أهمية تطوير إطار قانوني جديد يجمع بين الأمن السيبراني والمخاوف البيئية واحتياجات التشغيل لضمان سلامة واستدامة البنية التحتية المدارية.

ثالثاً: الإطار القانوني في المجال السيبراني

تتميز البيئة القانونية في المجال السيبراني بالتجزئة، مع تطور سريع يشمل مختلف الدول والمناطق. فقد وفرت اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، إضافة إلى المبادئ التوجيهية للاتحاد الدولي للاتصالات (ITU)، حماية جزئية للبيانات والخصوصية والتنقل العابر للحدود للمعلومات (شيرمان، 2021). كما حاول فريق الخبراء الحكوميين التابع للأمم المتحدة (UN GGE) تقديم معايير طوعية لسلوك الدولة في الفضاء السيبراني، مع التركيز على السيادة وعدم التدخل والمساءلة (بهات، 2025). ورغم هذه الجهود، يظل تحدي الإنفاذ كبيرًا نظرًا لاختلاف السياسات الوطنية تجاه معايير السيادة الرقمية والأمن السيبراني. وقد بدأت الدول العربية تدريجيًا في تبني قوانين محلية للأمن السيبراني تتوافق مع المعايير الدولية للحفاظ على سيادتها الوطنية (عبد الرحمن، 2022). ويعتقد الباحثون أن تعزيز التعاون الرقمي عبر جامعة الدول العربية قد ساهم في تحسين مرونة الأنظمة وتقليل نقاط الضعف أمام الهجمات الإلكترونية العابرة للحدود (يوسف، 2020).

التحليل القانوني المقارن

يشير التحليل المقارن إلى أن أنظمة الحوكمة في المجالات البحرية والفضائية والسيبرانية، رغم تشابه أهدافها في إرساء الاستقرار، وتعزيز التعاون، وضمان الاستخدام السلمي، تختلف من حيث التقاليد القانونية وآليات الإنفاذ (Guilfoyle et al., 2022). فبينما تمنح اتفاقية الأمم المتحدة لقانون البحار الدول سيادة إقليمية وقضائية، تعزز معاهدة الفضاء الخارجي مفهوم الإشراف الجماعي على موارد مشتركة عالمية. أما الفضاء السيبراني فيظل غير منظم إلى حد كبير، ويفتقر إلى المعايير الملزمة والسياسات الإقليمية (شيرمان، 2021).

وتترتب على هذه الفروقات هيكليًا تداخلات وتناقضات واضحة، مثل الكابلات البحرية والأقمار الصناعية التي تحمل البيانات، لكنها تخضع لقوانين حماية مختلفة، دون وجود مبادئ حماية موحدة قانونيًا. وعلاوة على ذلك، بينما تكون المعاهدات البحرية والفضائية ملزمة للدول، فإن الحوكمة السيبرانية غالبًا ما تحوّل المساءلة إلى الجهات الفاعلة غير الحكومية، ما يؤدي إلى غموض المساءلة. ومن دون إطار قانوني دولي موحد، فإن البنية التحتية الرقمية الحيوية تبقى معرضة للتهديدات الهجينة، وقد تُستغل كأداة ضغط سياسية (حمدي، 2024؛ يوسف، 2020). لذلك، هناك حاجة ماسة إلى استراتيجية قانونية مشتركة توازن بين السيادة الوطنية والترابط العالمي، وتعزز تبادل المعلومات، وتوفر معايير دولية قابلة للتنفيذ لحماية البنية التحتية الرقمية عبر مختلف الولايات القضائية.

المبحث الثاني: الإشكالات البنيوية ومنهجية تحليل التهديدات في البنية التحتية الرقمية الحيوية

المطلب الأول: التهديدات ونقاط الضعف في البنية التحتية الرقمية الحيوية

أصبح الدفاع عن البنية التحتية الرقمية العالمية يمثل بيئة معقدة متعددة الأبعاد، تشمل تهديدات تقليدية، وسيبرانية، وهجينة. تتعرض مراكز البيانات والكابلات تحت سطح البحر والأقمار الصناعية، التي تشكل الجهاز العصبي للاقتصاد العالمي، لهجمات من قبل جهات فاعلة حكومية وغير حكومية. ويعد فهم طبيعة هذه المخاطر وتطورها أمراً ضرورياً لتعزيز القانون الدولي وأطر الحوكمة التي تحمي البنية التحتية الحيوية (يوسف، 2020).

التهديدات التقليدية:

ترتبط التهديدات التقليدية للبنية التحتية الرقمية بالتخريب المادي، والتجسس، والمخاطر البيئية. فقد واجهت الكابلات تحت سطح البحر مخاطر السحب بواسطة المراسي، وشباك صيد الجر، وحتى القطع المتعمد الذي قد يعطل الشبكات المالية والاتصالات العالمية. وتشير Wasiuta (2023) إلى أن هذه الكابلات تمثل واحدة من أقل العناصر حمايةً وأكثرها أهمية ضمن شبكة الاتصال العالمية، مع وجود عدد محدود من آليات الإنفاذ في البحر. وبالمثل، فإن الأقمار الصناعية تواجه مخاطر تصادم الحطام والانفجارات الإشعاعية الطبيعية التي تهدد سلامة الإشارات ونقل البيانات. كما تصاعدت المخاوف المتعلقة بالسيادة بسبب التجسس والتنصت على المراسلات السرية من قبل وكالات الاستخبارات، كما أظهرت أحداث المراقبة السابقة (العتيبي، 2023). وتساهم الظواهر الطبيعية، مثل الزلازل والانفجارات البركانية، في زيادة قابلية البنية التحتية للخطر، خاصة في مناطق المحيط الهادئ والبحر الأحمر، حيث تتركز كثافة الكابلات. وتوضح هذه المخاطر ضعف النظم الحالية، مثل اتفاقية الأمم المتحدة لقانون البحار، لافتقارها إلى آليات إنفاذ فعالة لمواجهة التخريب المتعمد أو التجسس.

التهديدات السيبرانية:

تتسم الهجمات على البنى التحتية السيبرانية بالتطور والانتشار الواسع، وتشكل مؤشرات على تسليح الفضاء السيبراني من قبل جهات حكومية وغير حكومية. وفقاً لكومار (2023)، غالباً ما تستهدف الوكالات التابعة للدول مرافق إنزال الكابلات تحت سطح البحر ومراكز البيانات لتعطيل الخدمات أو جمع المعلومات الاستخباراتية. ويؤكد Paik (2025) أن هذه الهجمات تشكل جزءاً من استراتيجيات جيوسياسية أوسع للتعطيل الرقمي، باعتبارها وسيلة فعالة من حيث التكلفة ويمكن إنكارها. ومن أوجه الضعف السيبراني المتزايدة في بعض المناطق العربية غياب السيطرة المتساوية على الخدمات الرقمية، نتيجة

انتشـــار الحوكمة الإلكترونية واســـتخدام الخدمات الســـحابية، مما جعل المنطقة أكثر عرضـــة للهجمات الإلكترونية، خاصة في البلدان ذات مستويات منخفضة من الأمن السيبراني المتقدم (2022، الفقرة 5). وقد أدى ذلك إلى نمو الهجمات الإلكترونية في هذه الدول نتيجة انتشـــار الخدمات الســـحابية، مما يبرز أهمية القانون العابر للحدود والتعاون الإقليمي للحفاظ على استمرارية البيانات وسلامتها.

التهديدات الهجينة:

تســتلزم التهديدات الهجينة تقارب الهجمات المادية والســيبرانية، حيث يتم دمج الهجمات الإلكترونية مع الهجمات الحركية. ومن الأمثلة على ذلك اســـتهداف خطوط أنابيب نورد ســـتريم وبلطيق كونكتور (Ng, 2025)، والتي تخلق منطقة رمادية بين الحرب التقليدية والســيبرانية، وتتســبب في تحديات قانونية تتعلق بالإسناد والتناسب ضمن القانون الدولي. وتشعر بعض الدول العربية بالتهديد من أشكال الهجمات الهجينة، بما في ذلك الصراعات الداخلية والتجسس السيبراني والمعلومات المضللة.

معضلة الاستخدام المزدوج:

تشكل معضلة الاستخدام المزدوج أحد أبرز التحديات في حماية البنية التحتية الرقمية، إذ إن الأنظمة والتقنيات تخدم أغراضاً مدنية وعسكرية على حد سواء. فتستخدم الأقمار الصناعية لمراقبة الطقس ولجمع بيانات الاســـتطلاع، فيما تســـتغل مراكز البيانات التي تحتوي على معلومات تجارية لأغراض التحليل الدفاعي. وفقاً لديميتروف (2025)، يضـاعف هذا التداخل من تعقيد المسـائل القانونية المتعلقة بضـمان حماية الأصـول المدنية والأهداف العسـكرية المشـروعة. ويشـير الخيام (2021) إلى أن الغموض المرتبط بالأنشـــطة ذات الاســـتخدام المزدوج في الفضـــاء يخلق حالة من عدم اليقين في تطبيق معاهدة الفضـــاء الخارجي، خصوصاً فيما يتعلق باستخدام الأقمار الصناعية العسكرية واختبارات الأسلحة المضادة للأقمار الصـــناعية. وبالمثل، تواجه البنية التحتية البحرية ذات الاســـتخدام المزدوج تحديات كبيرة في تعزيز وتنظيم الممارسات المشروعة ضمن المياه الدولية.

المطلب الثاني: منهجية البحث

يتناول هذا المطلب المنهجية المعتمدة في البحث عن فرص تعزيز حماية البنية التحتية الرقمية الحيوية، بما في ذلك الكابلات البحرية والأقمار الصـــناعية ومراكز البيانات، من خلال اســـتغلال أطر القانون الدولي وأدوات الحوكمة العالمية. وتهدف هذه المنهجية إلى تقديم تحليل شـــامل للأطر القانونية الدولية القائمة، والمعاهدات، والوثائق السـياسـاتية، ودراسـة نقاط القوة والضـعف والثغرات القانونية، بما يسـهم في تطوير استراتيجيات فعالة لحماية هذه البنية التحتية الحيوية.

تستند الدراسة إلى تصميم تحليلي تفسيري نوعي يركز على تفسير النصوص القانونية الدولية والمبادئ القانونية المعمول بها، وكذلك دراسة الحالة وتطبيق المقارنات بين الأنظمة المختلفة، بغية الكشف عن التناقضات والاختلافات في آليات الحوكمة والإنفاذ. ويتيح هذا النهج فهماً دقيقاً للتهديدات التقليدية والسيبرانية والهجينة، وتقييم مدى قدرة الأطر القانونية الحالية على التعامل معها، وتقديم توصيات لتطوير القوانين والمعاهدات بما يضمن استدامة البنية التحتية الرقمية.

تصميم البحث:

يعتمد البحث على تصميم نوعي تحليلي تفسيري، وهو الأنسب لدراسة القضايا القانونية والجيوسياسية المعقدة التي لا يمكن قياسها بطرق كمية. يسمح هذا التصميم بفهم المعاني المتضمنة في النصوص القانونية والمعاهدات الدولية، وتحليل تأثيرها على حماية البنية التحتية الرقمية. كما يوفر الإطار التحليلي التفسيري المرونة الكافية لدراسة التهديدات الهجينة والتحديات الجديدة التي تفتقر إلى سوابق قانونية واضحة، مثل الهجمات السيبرانية المتقدمة أو الهجمات المدمجة بين الفيزيائية والرقمية.

من خلال هذا الإطار، يتم تقييم فعالية الأنظمة القانونية المختلفة، مثل اتفاقية الأمم المتحدة لقانون البحار في المجال البحري، ومعاهدة الفضاء الخارجي في المجال الفضائي، واللائحة العامة لحماية البيانات (GDPR) في المجال السيبراني، على التوالي، في التعامل مع الثغرات القانونية المرتبطة بحماية البنية التحتية الحيوية.

السكان والعينة:

يتكون مجتمع البحث من الوثائق القانونية الدولية، المعاهدات، القرارات الدولية، التقارير الحكومية، والوثائق المؤسسية ذات الصلة بحماية البنية التحتية الرقمية. وقد تم اختيار العينة بعناية لضمان تمثيل شامل للأطر القانونية والسياساتية، وتغطية الجوانب البحرية والفضائية والسيبرانية.

وتشمل العينة العناصر التالية:

- الكابلات البحرية التي تخضع لأحكام اتفاقية الأمم المتحدة لقانون البحار (UNCLOS)، وبالأخص المواد 79 و113، التي تحدد حقوق وواجبات الدول فيما يتعلق بمد الكابلات وصيانتها وحمايتها.
- معاهدة الفضاء الخارجي لعام 1967، إلى جانب قرارات الأمم المتحدة ذات الصلة بالحطام الفضائي واختبارات الأسلحة المضادة للأقمار الصناعية (ASAT).
- اللائحة العامة لحماية البيانات (GDPR) والأطر التنظيمية للاتحاد الأوروبي، وتقارير فريق الخبراء الحكوميين التابع للأمم المتحدة (UN GGE) حول الأمن السيبراني.
- دراسات الحالة المتعلقة بتخريب خط أنابيب نورد ستريم، وحادثة موصل البلطيق، والهجمات الإلكترونية على مراكز البيانات العالمية وأنظمة الأقمار الصناعية.

يضـــمن هذا الاختيار تغطية شـــاملة للأبعاد القانونية والتشـــغيلية للبنية التحتية الرقمية عبر المجالات الثلاثة، ويتيح رصد التحديات القانونية والسياساتية الفريدة لكل مجال.

أدوات البحث وجمع البيانات:

تستخدم الدراسة تحليل المستندات القانونية والمقارنة القانونية كأدوات بحث رئيسية. يقوم تحليل الوثائق على مراجعة المنشـــورات الأكاديمية، تقارير الأمم المتحدة، الوثائق الحكومية، والمراجعات القانونية لتعريف الموضوعات والمبادئ القانونية والتفسيرات ذات الصلة. يتيح هذا التحليل تصور حماية البنية التحتية الرقمية من خلال أطر قانونية مختلفة، وفهم كيفية معالجة المخاطر التقليدية، السيبرانية، والهجينة.

كما يُســـتخدم القانون المقارن لفحص الاختلافات والتشـــابهات بين الأطر القانونية عبر المجالات المختلفة، على ســـبيل المثال مقارنة حماية الكابلات البحرية بنظم حماية الفضـــاء أو الحماية الســـيبرانية. ويشمل ذلك المراجع العربية، مثل أعمال عبد الرحمن (2022) والكيلاني (2021)، لتوضيح الصلة بين السيادة الرقمية العربية وأطر القانون الدولي للأمن السيبراني وحوكمة الفضاء.

الصلاحية والموثوقية:

لتعزيز صـــلاحية البحث وموثوقيته، تم اتباع اســـتراتيجيات متعددة، أبرزها تثليث مصـــادر المعلومات، حيث يتم مقارنة البيانات المستخلصة من الأدبيات العلمية، الوثائق القانونية الدولية، وتقارير السياسات الحكومية. ويتيح ذلك الحد من التحيز التفسيري، وضمان صحة النتائج المستخلصة. كما تم استخدام أساليب الترميز القانونية، والتفكير التحليلي، والمراجعة الدقيقة للمصادر الأكاديمية المحكمة، ومصادر الأمم المتحدة الرسمية، والبيانات الحكومية المؤكدة، لضمان موثوقية عالية للبيانات.

تحليل البيانات:

يعتمد تحليل البيانات على الترميز والتحليل المقارن لتصنيف وتفسير المعلومات المستخلصة. يتم إنشاء رموز تمثل موضـوعات مشـتركة، مثل الثغرات القانونية، السـيادة الرقمية، التهديدات الهجينة، والمسـؤولية المشتركة، ضمن النظم القانونية المختلفة. تُجمع هذه الرموز ضمن موضوعات أكبر للتحليل، ما يتيح تفسير المواد القانونية المعقدة بشكل منهجي ومنظم.

كما يســـتخدم التحليل المقارن لتحديد أوجه التشـــابه والاختلاف بين النظم البحرية والفضـــائية والسيبرانية، واكتشاف أوجه التآزر المحتملة لتطوير إطار حماية دولي موحد. وتعمل هذه العملية على تحديد الثغرات في المعاهدات الحالية وتقديم أســس قانونية لتطوير القوانين والشــراكات الجديدة لتعزيز حماية البنية التحتية الرقمية الدولية.

التطبيق القضائي:

يستعرض البحث بعض السوابق القضائية الدولية ذات الصلة بالبنية التحتية الرقمية والحيوية، لإظهار كيفية تطبيق القانون الدولي على حالات واقعية، بما يعكس الدور العملي للمعاهدات والأطر القانونية.

- أولاً، قضية Arctic Sunrise (هولندا ضد روسيا)، التي أيدت فيها محكمة التحكيم الدائمة مبدأ الضرورة في القانون الدولي العرفي، مما يسمح للدول الساحلية بالتصرف في المناطق الاقتصادية الخالصة لمواجهة تهديدات المخاطر البيئية. ويمكن تعميم هذا المبدأ على حماية الكابلات البحرية من التخريب المتعمد. ويبرز البحث أيضًا دور المادة 58 من اتفاقية الأمم المتحدة لقانون البحار في الإنفاذ عند مواجهة تهديدات هجينة، مع الإشارة إلى أن المحاكم قد تطبق أحكام المواد الأخرى، مثل المادة 194، لحماية البيئة والبنية التحتية البحرية (Hybrid CoE, 2025; Lott, 2025).
- ثانياً، قضية Schrems ضد (Facebook Ireland-18/311، 2020)، التي ألغت فيها محكمة العدل الأوروبية برامج نقل البيانات بين الاتحاد الأوروبي والولايات المتحدة بسبب عدم كفاية الضمانات ضد التجسس. يوضح هذا القرار تطبيق مبادئ اللائحة العامة لحماية البيانات على مراكز البيانات، ويؤكد على ضرورة تقييم المخاطر السيبرانية بشكل صارم، بما يفرض على الدول والمؤسسات الالتزام بالمعايير الدولية لحماية البيانات (Ferretti, 2024).

هذه الأمثلة القضائية تسلط الضوء على أهمية التفسير الديناميكي للقوانين والمعاهدات الدولية، وتوضح كيفية سد الفجوات القانونية الناجمة عن التهديدات التقليدية والسيبرانية والهجينة، وتأكيد دور الشراكات الدولية في حماية البنية التحتية الحيوية والرقمية.

الخاتمة:

أولاً: الاستنتاجات

خلص البحث إلى مجموعة من النتائج المهمة حول فعالية القانون الدولي في حماية البنية التحتية الرقمية الحيوية، بما في ذلك الكابلات تحت سطح البحر، والأقمار الصناعية، ومراكز البيانات. أظهرت النتائج أن النظام القانوني الدولي الحالي يعاني من عدد من العيوب الأساسية التي تحد من قدرته على مواجهة التهديدات المعاصرة والمتعددة الأبعاد. على الرغم من ازدياد الترابط بين المجالات البحرية والفضائية والسيبرانية، تظل المعاهدات الدولية منفصلة وغير متناسقة، وتفتقر إلى آليات إنفاذ موحدة وتنسيق فعال بين الهيئات الدولية (Bueger & Liebetrau, 2021; Pleasic, 2024).

تم تحليل البيانات وتصنيفها ضمن ثلاثة مجالات رئيسية: الثغرات القانونية، نقاط الضعف في السياسة، وقضـــايا الحوكمة الناشـــئة. وقد أبرزت النتائج أن اتفاقية الأمم المتحدة لقانون البحار ومعاهدة الفضـــاء الخارجي واللائحة العامة لحماية البيانات توفر تغطية جزئية فقط، لكنها تفتقر إلى آليات إنفاذ فعالة، ما يترك الكابلات البحرية والأقمار الصـــناعية ومراكز البيانات عرضـــة للهجمات المتعمدة أو الســـيبرانية أو الهجينة.

أظهرت الدراسة أن الثغرات القانونية تتجلى في غياب المساءلة والإجراءات التوضيحية بشأن التخريب والتجسس، وأن المعاهدات الحالية كتبت قبل العصر الرقمي ولا تعكس التحديات المعاصرة (Pleasic, 2024). فعلى ســـبيل المثال، المادة 113 من اتفاقية الأمم المتحدة لقانون البحار تحدد الجريمة الجنائية المتمثلة في الإضـــرار المتعمد بالبرقيات، لكنها تترك التنفيذ للدول، ما يمنحها ســـلطة محدودة. وفي المجال الفضائي، لا توفر معاهدة الفضاء الخارجي آليات واضحة للتحكم في استخدام الأسلحة المضادة للأقمار الصـــناعية أو لتتبع الحطام الفضـــائي، مما يخلق غموضـــاً قانونياً عند حدوث هجمات هجينة أو ســـرية (Blechová, 2025).

أما على مستوى السياسات، فتبرز نقاط الضعف في انقسام الحوكمة الدولية بين هيئات منفصلة لكل مجال، ما يعيق التنسيق ويخلق تداخلات في السلطات القضائية. كما يؤدي التفاوت في تطبيق المعايير إلى حماية غير متسقة للبنية التحتية الرقمية عبر الولايات القضائية، خاصة في الدول النامية، بما فيها بعض الدول العربية والأفريقية، حيث لا تزال السياسات الأمنية قديمة أو جزئية (Ng, 2025؛ عبد الرحمن، 2022).

وتؤكد نتائج البحث أن البنية التحتية الرقمية تتميز بطبيعة الاســـتخدام المزدوج، إذ يمكن اســـتخدام الأقمار الصـناعية أو الكابلات البحرية لأغراض مدنية وعسـكرية على حد سـواء، ما يعقد تطبيق القانون الدولي الإنساني ويزيد من صعوبة مساءلة المسؤولين عن الهجمات.

في ضـــوء ذلك، يبدو جلياً أن البنية التحتية الرقمية تحتاج إلى حماية متكاملة تتجاوز الفضـــاء القانوني التقليدي، لتأمين الســـلام والاســـتقرار والســـيادة العالميين، وضـــمان قدرتها على الصـــمود أمام التهديدات الهجينة والعابرة للحدود (Mattson & Larson, 2023؛ حمدي، 2024).

التوصيات:

ولمعالجة أوجه القصور القانونية والمؤسسية التي كشفت عنها الدراسة، تُقدّم التوصيات التالية:

- تعديل اتفاقية الأمم المتحدة لقانون البحار:

ينبغي إدراج التزامات واضحة للحماية الجماعية للبنية التحتية البحرية، بحيث يصبح التعاون بين الدول في الحد من مخاطر التخريب والهجمات الهجينة ضـــد الكابلات البحرية والبنية التحتية المرتبطة بها إلزاميًا قانونيًا. ويمكن تعزيز الإنفاذ من خلال تطوير أنظمة مراقبة مشـــتركة، ومبادئ توجيهية إقليمية للاســـتجابة السريعة للحوادث، مع تحديد آليات واضحة للمساءلة القانونية.

- إنشاء وكالة عالمية لحماية البنية التحتية الرقمية (GDIPA):

من الضروري تأسيس هيئة دولية تنسق بين الاتحاد الدولي للاتصالات، والمنظمة البحرية الدولية، ولجنة استخدام الفضاء الخارجي للأغراض السلمية، بحيث توفر منصة موحدة لمراقبة البنية التحتية الرقمية، وتبادل المعلومات الاستخباراتية، والاستجابة الفورية للحوادث على امتداد السلسلة المتصلة بين البحر والفضاء والمجال السيبراني، بما يعزز القدرة على التعامل مع الهجمات العابرة للحدود.

- تعزيز التعاون الإقليمي العربي في الأمن السيبراني:

يمكن للدول العربية، استنادًا إلى عبد الرحمن (2022) وحمدوي (2024)، تطوير نظام مشترك للأمن السيبراني عبر مواءمة التشريعات، وإجراء تدريبات مشتركة، وتنفيذ مشاريع لبناء القدرات تهدف إلى حماية الكابلات البحرية ومراكز البيانات في المنطقة، بما يســـهم في تحقيق مســـتوى متوازن من الحماية الرقمية بين الدول.

- تبني الحوكمة التعاونية والاستباقية:

يجب أن تتجاوز اســـتراتيجيات الحوكمة الحدود القضـــائية والقطاعية، بحيث تضـــمن مشـــاركة الدول الكبرى والنامية على حد سـواء في صـنع القرار العالمي، مع الالتزام بمبادئ الشـفافية، والمسـؤولية الجماعية، والحياد التكنولوجي، لضمان قدرة النظام الدولي على الاستجابة الفعالة للتهديدات الرقمية المعقدة.

- التركيز على الاتجاهات المستقبلية والتقنيات الحديثة:

يجب توجيه البحوث وصـنع السـياسـات نحو تطوير أنظمة مراقبة قائمة على الذكاء الاصـطناعي قادرة على اكتشـــاف الحالات الشـــاذة في البنية التحتية الرقمية في الوقت الفعلي، من خلال الجمع بين صـــور الأقمار الصـناعية، والتتبع البحري، وتحليلات بيانات الشـبكة، للوقاية من التخريب والهجمات الإلكترونية قبل التصـعيد. كما ينبغي دمج عوامل المرونة البيئية، مثل تأثير التغير المناخي والنشـاط الزلزالي تحت سـطح البحر، لضمان استدامة وأمان الشبكات الرقمية العالمية.

المراجع:

حمدي، علي (2024). التحول الرقمي والأمن القومي العربي. بيروت: المركز العربي للأبحاث ودراسة السياسات.

العتيبي، ناصر (2023). القانون الدولي وحماية الكابلات البحرية. الرياض: جامعة الملك سعود.

عبد الرحمن، خالد (2022). الأمن السيبراني والبنية التحتية الرقمية في العالم العربي. القاهرة: مركز الدراسات الاستراتيجية.

الكيلاني، محمد (2021). الفضاء الخارجي والتحديات القانونية للأقمار الصناعية. عمّان: دار وائل للنشر.

يوسف، سامر (2020). البنية التحتية الحيوية في الأمن الدولي المعاصر. دمشق: دار الفكر.

Bhatt, P. (2025). Data as Sovereign Rights and UNCLOS: Protection of Undersea Cables through Legislative Mechanisms. OPR, 216. Retrieved from https://www.marseccoe.org/wp-content/uploads/2025/03/4th-Maritime-Security-Proceedings.pdf#page=220.

Blechová, A. (2025, May). The Next Step in Global Connectivity: Legal Challenges in the Shift from Subsea Cables to Satellites. In 2025 17th International Conference on Cyber Conflict: The Next Step (CyCon) (pp. 39–55). IEEE. https://ieeexplore.ieee.org/abstract/document/11103582/.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129.

Bueger, C., Liebetrau, T., & Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. Report for SEDE Committee of the European Parliament, PE702, 557, 11–56.

Dimitrov, T. (2025). Critical Maritime Infrastructure Protection. Strategies XXI, 389. https://www.ceeol.com/content-files/document-1431664.pdf.

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine cables and the risks to digital sovereignty. Minds and Machines, 34(3), 31. https://link.springer.com/article/10.1007/s11023-024-09683-z.

10. Guilfoyle, D., Paige, T. P., & McLaughlin, R. (2022). The final frontier of cyberspace: The seabed beyond national jurisdiction and the protection of submarine cables. International & Comparative Law Quarterly, 71(3), 657–696. https://doi.org/10.1017/S0020589322000282.

Kavanagh, C., Franken, J., & He, W. (2025). Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure. Geneva, Switzerland: UNIDIR. https://unidir.org/wp-content/uploads/2025/04/UNIDIR_Achieving_Depth_Subsea_Telecommunications_Cables_Critical_Infrastructure.pdf.

Kumar, R. (2023). Securing the Digital Seabed: Countering China's Underwater Ambitions. Journal of Indo-Pacific Affairs, 6(8). https://media.defense.gov/2023/Nov/14/2003340185/-1/-1/1/FEATURE%20KUMAR%20-%20JIPA.PDF.

Mattsson Larsson, N. (2023). Protection of Digital Infrastructures in Areas Beyond National Jurisdiction in International Law. University of Gothenburg. https://gupea.ub.gu.se/handle/2077/74735.

Ng, J. R. (2025). The Role of Underwater Cables in Global Geopolitics. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5169546.

Paik, A. (2025). Protecting Undersea Cables and South Korea’s Role. The Washington Quarterly, 48(2), 77–91. https://doi.org/10.1080/0163660X.2025.2518647.

Pleasic, S. B. (2024). Securing Subsea Cable Critical Infrastructure: Holes in the Governing Legal Framework in the United States and Internationally. Seton Hall University. https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2438&context=student_scholarship.

Sherman, J. (2021). Cyber defense across the ocean floor: The geopolitics of submarine cable security. Washington, DC: Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf.

Tréhu, J., & Roberts, M. (2024). Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective. Instituto Affari Internazionali, 28. https://www.gmfus.org/sites/default/files/2024-03/iaip2404.pdf.

20. Wasiuta, O. (2023). Russian threats to the submarine internet cable infrastructure. Zeszyty Naukowe SGSP / Szkoła Główna Służby Pożarniczej.

https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-6a870221-de18-4e53-a081-c820e4d8242e.

Lott, A. (2025). Unconventional legal approaches to protecting underwater infrastructure. The Hague Center for Strategic Studies. https://hcss.nl/wp-content/uploads/2025/03/Unconventional-Legal-Approaches-to-Protecting-Underwater-Infrastructure-HCSS-2025-1.pdf

Hybrid Center of Excellence. (2025). Protecting Marine Infrastructure from Hybrid Threats: Legal Options. Center of Hybrid Excellence. https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf

Ferretti, M. (2024). Legal Issues in Reconciling Data Protection Artificial Intelligence and Cybersecurity in the European Union. Missouri Law Review, 89 (4), 1023-1056. https://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=4681&context=mlr

IISD. (2025). Cybersecurity and International Trade. International Institute for Sustainable Development. https://www.iisd.org/system/files/2025-08/cybersecurity-international-trade-policy.pdf

26. O'Meara, R. (2024). Anti-satellite weapons and self-defence: law and restrictions. NATO's Center of Excellence for Cooperative Cyber Defense. https://ccdcoe.org/uploads/2024/05/CyCon_2024_OMeara-1.pdf.