UNIVERSITÉ DU QUÉBEC À MONTRÉAL -
INSTITUT D'ÉTUDES POLITIQUES DE GRENOBLE

LA GUERRE INVISIBLE DES CÂBLES : SABOTAGES ET MENACES EN MER DE CHINE MÉRIDIONALE

TRAVAIL DE FIN D'ÉTUDES
PRÉSENTÉ COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE, PROFIL DOUBLE DIPLÔME IEPG

PAR
CAMILLE LATY

NOVEMBRE 2025

f

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

Table des matières

LISTE DES ABRÉVIATIONS, DES SIGLES ET ACRONYMES

AAE-1 – Asia-Africa-Europe-1
AAG – Asia-America Gateway
AIS – Automatic Identification System / Système d'identification automatique
APG – Asia Pacific Gateway
ASEAN – Association of Southeast Asian Nations / Association des nations de l'Asie du Sud-Est
BRI – Belt and Road Initiative / Nouvelle route de la soie
DSR – Digital Silk Road / Route de la soie numérique
GAFAM – Google, Apple, Facebook, Amazon & Microsoft
MCM – Mer de Chine méridionale
MCT – Malaysia-Cambodia-Thailand
NSA – National Security Agency
OTAN – Organisation du Traité de l'Atlantique Nord
SJC – Southeast Asia-Japan
SMW3 – Southeast Asia - Middle East - Western Europe 3
SMW5 – Southeast Asia - Middle East - Western Europe 5
TIC – Technologies de l'information et de la communication
TLSSC – Timor-Leste South Submarine Cable
TPE – Trans Pacific Express
UNCLOS – United Nations Convention on the Law of the Sea / Convention des Nations unies sur le droit de la mer
UUVs – Unmanned undersea vehicles / Véhicules sous-marins sans pilote
ZEE – Zone économique exclusive

RÉSUMÉ

Les câbles sous-marins de télécommunications sont des infrastructures critiques et stratégiques qui assurent la transmission de données Internet essentielles au bon fonctionnement de toute société interconnectée. Ces dernières années, les actes de sabotage visant ces câbles ont augmenté. En 2023 et 2025, les incidents survenus à Taïwan ont attiré l'attention sur cette tendance émergente qui s'inscrit dans les méthodes dites « en zone grise ». Or, la littérature scientifique porte peu d'attention aux attaques volontaires soutenues ou perpétrées par un État contre ces câbles, et encore moins aux réactions des acteurs visés par ces actes de sabotage. Ce travail de recherche contribue donc à combler cette lacune en étudiant les cas survenus en Asie du Sud-Est, en mer de Chine méridionale et, plus particulièrement, à Taïwan. Les cas taïwanais sont marqués par de sérieux soupçons envers la Chine comme auteur des dommages, illustrant ainsi les méthodes chinoises en zone grise, mais aussi la concurrence numérique sino-américaine dans la région. Les fonds marins deviennent ainsi de plus en plus le théâtre de la compétition entre les grandes puissances. Cela souligne la nécessité d'étudier les stratégies de sécurisation des câbles dans un contexte international où la supériorité technologique et le contrôle de l'information sont des enjeux stratégiques. À travers une synthèse des connaissances, il sera démontré que les câbles sous-marins sont désormais perçus non seulement comme des infrastructures critiques devant être protégées contre des menaces extérieures, mais également comme des vecteurs d'influence et de menace.

Mots-clés : câbles sous-marins, infrastructures critiques, télécommunications, Internet, Asie du Sud-Est, mer de Chine méridionale, Taïwan, zone grise, enjeux stratégiques.

INTRODUCTION

L'infrastructure physique d'Internet est le symbole d'un monde de plus en plus digital et numérisé, dont l'interconnexion dépend d'un vaste réseau de câbles sous-marins.[1] Les câbles sous-marins sont des liaisons de communication à haut débit qui transmettent des données Internet sur de longues distances.[2] Aujourd'hui, un réseau de plus de 1,7 million de kilomètres de câbles à fibres optiques traverse les océans[3], permettant le partage de communications privées, de données commerciales et de renseignements de nature gouvernementale.[4] La toile numérique mondiale est composée de plus de 500 câbles sous-marins de télécommunications qui assurent la circulation de 98 % des données internationales.[5] Dans les prochaines années, la dépendance mondiale envers ces câbles est estimée augmenter en raison, entre autres, de l'utilisation croissante d'Internet, de l'importance du stockage en nuage, du développement des réseaux 5G et de l'intelligence artificielle.[6] Ainsi, les câbles sont les principales infrastructures physiques et matérielles du cyberespace, sur lesquelles toutes sociétés interconnectées reposent. Une perturbation du réseau comporte un risque d'interruption ou de réduction des activités numériques quotidiennes.[7] Compte tenu de la dépendance mondiale à l'égard de ces infrastructures critiques, il est pertinent d'étudier les risques et les menaces qui pèsent sur les câbles sous-marins de télécommunications, en particulier les perturbations volontaires causées par un acteur étatique.

---

[1] Swinhoe, D. (2021, 26 août). What is a submarine cable? Subsea fiber explained. *Data Centre Dynamics (DCD)*. <https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/>.

[2] Annathurai, R. M. (2023). Battles below: Submarine Cables in Naval Warfare and International Humanitarian Law. Symposium Maritime Operations and Humanitarian Considerations. <https://www.researchgate.net/publication/377629871_BATTLES_BELOW_SUBMARINE_CABLES_IN_NAVAL_WARFARE_AND_INTERNATIONAL_HUMANITARIAN_LAW_Session_1_International_Humanitarian_Law_Naval_Operations>, p. 2.

[3] Ganz, A. *et al*. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines, 34*(31), 1-23. <https://doi.org/10.1007/s11023-024-09683-z>, p. 1.

[4] Beyer, J. L. *et al*. (2025). *Hidden Highways of the Internet: Global Subsea Cable Security* [Task Force Report]. Henry M. Jackson School of International Studies, University of Washington. <https://jsis.washington.edu/wordpress/wp-content/uploads/2025/03/Task-Force-B-Final-Report.pdf>, p. 1.

[5] Morel, C. (2023). L'Asie du Sud-Est, nouveau centre de gravité des câbles sous-marins. Dans *L'Asie du Sud-Est 2023 : bilan, enjeux et perspectives* (p. 73-109). Institut de recherche sur l'Asie du Sud-Est contemporaine (IRASEC). <https://doi.org/10.4000/books.irasec.6391>, p. 73.

[6] Bueger, C. et 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>, p. 391.

[7] Morel, C. (2015). Stratégie maritime – Le réseau mondial de câbles sous-marins : une toile dans la Toile. *Revue Défense Nationale, 784*(9), 117-120. <https://doi.org/10.3917/rdna.784.0117>, p. 117.

La rupture intentionnelle de câbles comme stratégie militaire n'est pas un phénomène nouveau. Les ancêtres des câbles sous-marins, c'est-à-dire les câbles télégraphiques, étaient également visés. Le premier câble a été posé en 1850 pour connecter le Royaume-Uni à l'Europe continentale et ainsi permettre les communications télégraphiques.[8] Le premier cas de coupure intentionnelle de câbles est survenu lors du conflit opposant les États-Unis à l'Espagne en 1898. À la suite de cet incident, les actes militaires visant ces infrastructures sont devenus de plus en plus courants.[9] Lors de la Première Guerre mondiale, des câbles télégraphiques étaient volontairement sectionnés afin de perturber les communications de l'adversaire et obtenir un avantage stratégique.[10] Pendant la Seconde Guerre mondiale, les câbles sous-marins de communication de l'Allemagne ont été rompus dans le but de l'isoler.[11] Lors de l'opération en Libye en 2011, des navires de l'Organisation du Traité de l'Atlantique Nord (OTAN) ont coupé des câbles sous-marins, provoquant l'interruption des télécommunications.[12] Ces exemples expriment l'importance stratégique des câbles sous-marins en tant qu'infrastructures de télécommunications essentielles. Plus récemment encore, des câbles ont été endommagés dans la mer Baltique en novembre 2024. Le navire chinois Yi Peng 3 aurait sectionné des câbles reliant la Finlande, la Suède, l'Allemagne et la Lituanie, suscitant également des soupçons de collusion avec la Russie. Les derniers incidents ont eu lieu à Taïwan, où des navires chinois ont endommagé des câbles sous-marins en janvier et en février 2025.[13] Taïwan est particulièrement concerné par ces enjeux, l'archipel ayant déjà été affecté par des coupures similaires en février 2023.[14] Si ces derniers exemples n'illustrent pas une coupure de câbles dans le contexte d'un conflit armé, ils témoignent d'une tendance croissante à utiliser ce type de tactique dans les opérations dites « en zone grise »[15], démontrant ainsi l'intérêt stratégique croissant des câbles sous-marins dans les conflits contemporains.

---

[8] Brake, D. (2019). Submarine Cables: Critical Infrastructure for Global Communications. *Information Technology and Innovation Foundation (ITIF)*, 1-11. <https://www2.itif.org/2019-submarine-cables.pdf>, p. 1.
[9] Morel, C. (2016). Menace sous les mers : les vulnérabilités du système câblier mondial. *Hérodote, 163*(4), 33-43. <https://doi.org/10.3917/her.163.0033>, p. 39.
[10] Racho, T. (2022). Les câbles sous-marins, des infrastructures internet critiques. *La revue européenne des médias et du numérique*, (61-62). <https://la-rem.eu/2022/10/les-cables-sous-marins-des-infrastructures-internet-critiques/>.
[11] Morel, C. (2016), *Op. cit.*, p. 39.
[12] Racho, T., *Op. cit.*
[13] Ocon, J. et Walberg, J. (2025). China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities. *Global Taiwan Institute, 10*(11), 9-12. <https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/>, p. 10.
[14] Beyer, J. L. *et al*., *Op. cit.*, p. 19.
[15] Burdette, L. (2024, 21 novembre). *What To Know About Submarine Cable Breaks*. TeleGeography. <https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks>.

Le présent travail se concentre sur l'Asie du Sud-Est et la mer de Chine méridionale (MCM), car cette région est particulièrement concernée par le sujet. Au cours de la dernière décennie, la construction soutenue de câbles sous-marins dans la zone indo-pacifique reflète l'essor économique de cette région.[16] Environ 60 câbles parcourent l'Asie du Sud-Est, formant ainsi un réseau dense et concentré au centre de l'Indo-Pacifique.[17] Fondée en 1967, l'Association des nations de l'Asie du Sud-Est (ASEAN – Association of Southeast Asian Nations) est une organisation politique, économique et culturelle composée de dix États membres, soit l'Indonésie, la Malaisie, les Philippines, Singapour, la Thaïlande, le Brunei, le Vietnam, le Laos, le Myanmar et le Cambodge.[18] Avec environ 125 000 nouveaux utilisateurs d'Internet par jour, les pays de l'ASEAN représentent l'un des marchés numériques dont la croissance est la plus rapide. La MCM est la route principale et la voie la plus efficace pour connecter les pays de l'ASEAN au reste du monde. Cependant, les tensions existantes et les revendications territoriales divergentes nuisent au développement du réseau de câbles sous-marins en MCM. Les différends territoriaux se sont intensifiés au cours des dix dernières années, notamment en raison de l'augmentation des actes d'affirmation de souveraineté commis par la Chine. L'Asie du Sud-Est et la MCM sont également le théâtre des rivalités sino-américaines et un terrain de compétitions technologiques stratégiques. Les câbles sous-marins se retrouvent ainsi au cœur des enjeux stratégiques et géopolitiques actuels dans la région sud-est asiatique. Or, si la concurrence numérique dans cette région fait l'objet de nombreuses recherches, peu d'entre elles se concentrent spécifiquement sur les câbles sous-marins.[19] Pour ces raisons, le présent travail se concentre sur les perturbations intentionnelles des câbles sous-marins en Asie du Sud-Est et en MCM.

Malgré l'importance du sujet, Bueger et Liebetrau soulignent le manque d'attention accordée aux réseaux de câbles par la communauté scientifique dans les domaines sécuritaire, géopolitique et de la gouvernance mondiale. À l'inverse de la communauté scientifique dans ces domaines, les grandes entreprises de technologie et les puissances étatiques – en particulier les États-Unis, la

[16] McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. *Australian Journal of International Affairs, 76*(2), 161-177. <https://doi.org/10.1080/10357718.2022.2051427>, p. 162.
[17] Morel, C. (2023), *Op. cit.*, p. 73.
[18] ASEAN Secretariat. (2025). *About us*. ASEAN Main Portal. <https://asean.org/about-us/>.
[19] Desurmont, J.-M. (2024, 21 mai). *Territorial Claims and Subsea Cables: The Geopolitics of Invisible Lines in the South China Sea*. Bloomsbury Intelligence & Security Institute (BISI). <https://bisi.org.uk/reports/territorial-claims-and-subsea-cables-the-geopolitics-of-invisible-lines-in-the-south-china-sea>.

Chine et la Russie – portent, quant à eux, une attention croissante envers l'importance stratégique du réseau de câbles sous-marins dans le cadre de la concurrence numérique actuelle.[20] Même si la littérature traitant du sujet est limitée, un consensus semble exister au sein de la communauté scientifique. En effet, plusieurs auteurs dont Morel, Namor, Annathurai ainsi que Bueger et Liebetrau précisent que la littérature porte peu d'attention aux attaques volontaires contre le réseau de câbles sous-marins, alors que son caractère essentiel reflète pourtant un risque plus élevé d'être pris pour cible. De plus, la réaction des États dont les câbles ont été sabotés intentionnellement par un autre État fait l'objet de peu d'attention.[21] Cette situation s'explique en partie par la difficulté d'attribution, c'est-à-dire la difficulté à identifier la cause et l'intentionnalité d'une rupture. La difficulté d'attribution est une caractéristique inhérente aux menaces relatives aux câbles, en particulier lorsque la responsabilité d'un État est soupçonnée dans le sabotage d'un câble sous-marin.[22] Par ailleurs, la plupart des études existantes dans le domaine de la sécurité adoptent une perspective transatlantique émanant de l'OTAN, ce qui inclut souvent une perception de la menace provenant principalement de la Russie.[23] Cette perspective nord-atlantique est restrictive et souligne la nécessité pour la communauté scientifique de se pencher sur le sujet. Le premier objectif de ce travail est de contribuer à combler certaines lacunes identifiées dans la littérature, à savoir le manque d'attention portée aux dommages intentionnels causés par un État et aux réactions des États visés, en particulier en Asie du Sud-Est et en MCM. En outre, les trois incidents suspects survenus à Taïwan, c'est-à-dire les événements des 2 et 8 février 2023, du 3 janvier 2025, puis du 25 février 2025, attirent l'attention sur la multiplication des perturbations de câbles sous-marins ces dernières années.[24] Ces trois incidents ont pour point commun les soupçons envers un acteur étatique, à savoir la Chine, comme auteur présumé de ces dommages. Le présent travail vise donc à répondre à la question de recherche suivante : comment est-ce que Taïwan réagit face au sabotage intentionnel de ses câbles sous-marins par la Chine ? Une attention particulière est portée aux méthodes en zone grise et aux cas survenus à Taïwan, car ceux-ci sont récents et font l'objet de sérieux soupçons à l'encontre d'un acteur étatique. Malgré son statut particulier, les incidents à Taïwan sont étudiés puisqu'ils permettent d'illustrer l'enjeu géopolitique relatif aux câbles sous-

[20] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 392.
[21] Morel, C. (2019). La mise en péril du réseau sous-marin international de communication. *Flux, 118*(4), 34-45. <https://doi.org/10.3917/flux1.118.0034>, p. 34-35.
[22] Bueger, C. et Liebetrau, T., *Op. cit.*; Beyer, J. L. *et al*., *Op. cit.*
[23] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 395.
[24] Beyer, J. L. *et al*., *Op. cit.*, p. 19-24.

marins dans la région. D'ailleurs, il n'est pas possible d'analyser les réactions de Taïwan sans prendre en compte les tensions géopolitiques préexistantes. Le second objectif de cette recherche est donc de comprendre comment les dynamiques de pouvoir et la concurrence numérique sino-américaine se manifestent dans le cas des câbles sous-marins à Taïwan, mais également en Asie du Sud-Est et en MCM de manière plus générale.

Au travers d'une synthèse des connaissances, il sera démontré que le cas des câbles sous-marins en Asie du Sud-Est et en MCM, et plus particulièrement à Taïwan, s'inscrit dans la rivalité numérique sino-américaine dans cette région, révélant une continuité des tensions géopolitiques déjà existantes. En outre, le travail permet de mettre en lumière des actes qui s'inscrivent dans les méthodes en zone grise, révélant ainsi une tendance émergente quant à l'instrumentalisation des câbles sous-marins de télécommunications dans ce genre de méthodes. Il sera également démontré que les câbles sous-marins sont désormais considérés non seulement comme des infrastructures critiques devant être protégées contre des menaces extérieures, mais également comme des vecteurs d'influence et de menace. Après une brève présentation de la méthode adoptée et des limites de la recherche, l'objet de l'étude est défini comme étant une infrastructure critique et stratégique. Cette première section permet également de détailler les vulnérabilités et les risques qui pèsent sur les câbles sous-marins de télécommunications. Une fois que les bases nécessaires à la compréhension du sujet sont établies, la seconde section effectue une revue de la littérature scientifique pour établir l'état des lieux sur le sujet et fournir le cadre théorique. Les concepts clés sont l'invisibilité des câbles, la concurrence numérique, la sécurisation et la zone grise. Enfin, l'étude examine les cas récents soupçonnés d'avoir été orchestrés par la Chine contre les câbles taïwanais, ce qui permet d'analyser l'enjeu selon le contexte géopolitique de l'Asie du Sud-Est et de la MCM.

MÉTHODOLOGIE

Dans le cadre de ce travail, une synthèse des connaissances permet de répondre à la question de recherche. La revue de la littérature scientifique établit l'état des lieux concernant l'étude sécuritaire des câbles sous-marins de télécommunications, plus particulièrement en Asie du Sud-Est et en mer de Chine méridionale. La revue des articles académiques permet également de déterminer le cadre théorique sur lequel se base l'analyse qualitative. Les concepts de zone grise, de sécurisation et de concurrence numérique soutiennent cette analyse, qui s'accompagne d'ailleurs d'exemples concrets accessibles au public. Les exemples d'incidents sont recueillis à partir de sources académiques et d'articles de journaux. De plus, le présent travail se concentre sur les acteurs étatiques, tout en reconnaissant l'influence du secteur privé sur les intérêts nationaux. Autrement dit, malgré l'influence mutuelle entre les secteurs public et privé, l'analyse se concentre sur les actions des États en raison de l'intérêt émergent porté par ces acteurs envers les câbles sous-marins. En outre, l'étude se concentre sur les actions directes visant le réseau physique de câbles, et non sur les actions indirectes qui visent l'information transitant par ces câbles.

L'une des principales limites de cette recherche relève de la confidentialité du sujet et du nombre très limité de cas confirmés de sabotage intentionnel par un État. En effet, l'aspect confidentiel de certaines questions relatives aux câbles sous-marins ne permet pas à cette recherche d'être complète. D'ailleurs, Morel évoque la même limite dans l'un de ses articles en précisant que le caractère parfois confidentiel relatif aux atteintes aux câbles, que ce soit de la part des acteurs publics ou privés, complexifie la compréhension du réseau câblé mondial.[25] Les limites de ce travail peuvent toutefois être explorées dans de futures recherches qui compléteraient celle-ci. Par exemple, il pourrait être pertinent d'inclure des entrevues avec des experts du sujet et de la région, ou encore avec des représentants gouvernementaux ou d'entreprises privées concernés par l'enjeu. Des sources primaires seraient particulièrement pertinentes compte tenu du caractère actuel et continu du sujet, permettant ainsi de rester informé des développements les plus récents. Une étude comparative entre divers cas serait également pertinente pour donner plus de profondeur à l'analyse. Une comparaison pourrait se pencher sur deux cas survenus dans des régions différentes du monde, car le nombre d'atteintes intentionnelles confirmées et commises par un État dans une

[25] Morel, C. (2019), *Op. cit.*, p. 36.

même région est limité. Une autre comparaison pourrait étudier les actions mises en place par deux États en réaction au sabotage perpétré par un même État tiers. De plus, le facteur linguistique réduit nécessairement le nombre de perspectives pouvant être présentées. Alors que le travail de recherche se concentre sur l'Asie du Sud-Est et la mer de Chine méridionale, les sources mobilisées sont en anglais ou en français. La langue constitue donc une limite supplémentaire, les articles académiques rédigés dans les langues locales ne pouvant être utilisés. En outre, cette étude ne se concentre pas sur l'état du droit international, le manque de réglementation ou encore les aspects techniques des câbles, mais plutôt sur les aspects sécuritaire et géopolitique. Ceci constitue une autre limite, car une approche pluridisciplinaire assurerait une perspective plus complète du sujet.

Dans le présent travail de recherche, le nombre de cas survenus en Asie du Sud-Est et en mer de Chine méridionale est très limité et ceux-ci concernent surtout Taïwan. C'est pourquoi l'analyse se concentre sur Taïwan en tant qu'acteur régional. Ce territoire n'est pas reconnu comme un État souverain sur la scène internationale, même s'il présente une volonté d'obtenir son indépendance par rapport à la Chine. Par pays indépendant, il est question d'une « collectivité humaine qui, sur un espace, s'est organisée […] sans subir l'organisation d'une autre – si ce n'est au sens de l'interdépendance ordinaire des unités politiques ».[26] En raison de son statut particulier, Taïwan ne dispose pas tout à fait des mêmes capacités que les États souverains.[27] Cette situation constitue une limite, car les réactions des États de la région ne peuvent pas être pleinement étudiées. Toutefois, le nombre très limité de ruptures intentionnelles de câbles sous-marins attribuables à un acteur étatique permet de justifier le choix de cet acteur régional, qui possède tout de même de nombreuses ressources stratégiques et une certaine indépendance politique.

[26] Detry, C.-E. (2023). *La résolution 2758 de l'AGNU et le statut de Taïwan en droit international*. Fondation pour la Recherche Stratégique (FRS). <https://www.frstrategie.org/sites/default/files/documents/programmes/Programme-Taiwan/2023/01-2023.pdf>, p. 8.
[27] *Ibid.*

1- LES CÂBLES SOUS-MARINS DE TÉLÉCOMMUNICATIONS

Cette section vise à définir l'objet de l'étude, à présenter des concepts clés et à poser les bases nécessaires à la bonne compréhension du sujet. Ces notions sont essentielles pour ensuite aborder la revue de la littérature et l'analyse du cas taïwanais. La première sous-section permet de comprendre les câbles sous-marins comme des infrastructures critiques et stratégiques, tout en abordant le concept d'interdépendance intersectorielle qui caractérise le réseau mondial câblé. La seconde sous-section décrit les vulnérabilités et les menaces auxquelles les câbles sont confrontés, tout en traitant d'une autre caractéristique du réseau, soit le concept de redondance.

Avant de passer à la première sous-section, il est nécessaire de décrire l'objet de l'étude. D'un point de vue physique, les câbles sous-marins ne sont généralement pas plus grands qu'un tuyau d'arrosage. Ces câbles à fibres optiques reposent dans les fonds marins et relient au moins deux points du réseau entre eux. Au centre des câbles se trouvent les fibres optiques, celles-ci étant recouvertes d'un gel de silicone, puis entourées de plusieurs couches de plastique, de fils d'acier, de cuivre et de nylon. Ces différentes couches assurent la protection du signal et du câble dans un environnement marin hostile, où il existe des risques de dommages causés par la faune, la pêche, les ancres ou encore les phénomènes naturels.[28] Près des côtes, les câbles sont enterrés afin d'assurer une protection supplémentaire. En eaux profondes, où les risques liés à la pêche et à la faune sont moins probables, les câbles reposent simplement sur les fonds marins sans être recouverts.[29] (*Voir la figure 1 en annexe pour une illustration de câble sous-marin*). La sous-section suivante définit les câbles sous-marins de télécommunications comme des infrastructures critiques et stratégiques.

1.1 Les câbles comme infrastructures critiques et stratégiques

Les infrastructures critiques peuvent être définies « comme l'ensemble des systèmes essentiels. Ainsi, les réseaux électriques, de télécommunications, d'eau, de gaz et de pétrole [...] sont considérés comme des infrastructures critiques. »[30] Les câbles de fibre optique sont des

[28] Swinhoe, D., *Op. cit.*; Beyer, J. L. *et al*., *Op. cit.*, p. 11.
[29] Brake, D., *Op. cit.*, p. 2.
[30] Rozel, B. (2009). La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances. Thèse, Institut polytechnique de Grenoble.

infrastructures critiques, car ils sont vitaux pour divers secteurs, tels que le commerce, la sécurité nationale, les opérations militaires et les communications civiles. Situés dans les fonds marins, ils jouent un rôle primordial dans les télécommunications mondiales et la connectivité Internet. Par exemple, les transactions financières internationales sont possibles grâce à Internet, qui permet le transit de 10 000 milliards de dollars quotidiennement. Les câbles sous-marins constituent donc le fondement de l'infrastructure mondiale d'Internet, ce qui en fait des infrastructures critiques.[31]

Morel précise que les attaques qui visent des infrastructures critiques ont le potentiel de paralyser l'ensemble de la société. Le concept d'interdépendance des réseaux explique que les menaces qui pèsent sur l'infrastructure de télécommunications, pèsent également sur les autres infrastructures critiques qui en dépendent.[32] L'interdépendance intersectorielle de ces infrastructures accroît le risque de crises simultanées, une attaque contre un câble sous-marin de télécommunications pouvant engendrer des conséquences néfastes sur d'autres infrastructures critiques.[33] Ce concept illustre l'avantage dont disposent les acteurs malveillants pour agir contre les infrastructures essentielles, y compris le réseau de câbles sous-marins, afin de maximiser efficacement les conséquences de leurs actions.[34] De plus, la reconnaissance des liaisons sous-marines comme des infrastructures critiques implique une collaboration accrue entre les secteurs public et privé pour assurer leur protection.[35]

Les câbles sous-marins sont également utilisés depuis longtemps à des fins militaires, que ce soit pour assurer les télécommunications entre bases militaires, pour collecter des renseignements par surveillance acoustique, ou encore pour assurer les communications directes bilatérales entre gouvernements.[36] Alors que les opérations militaires dépendent de plus en plus des infrastructures de communication, le risque que les câbles soient pris pour cible afin d'en tirer un avantage

[31] Annathurai, R. M., *Op. cit.*, p. 4.
[32] Morel, C. (2016), *Op. cit.*, p. 37.
[33] Morel, C. (2018). Protéger nos infrastructures vitales pour assurer notre résilience : les câbles sous-marins, entre invisibilité et vulnérabilité. *Les Champs de Mars, 30*(1), 419-426. <https://doi.org/10.3917/lcdm.030.0419>, p. 420.
[34] Morel, C. (2016), *Op. cit.*, p. 38.
[35] Morel, C. (2018), *Op. cit.*, p. 421.
[36] Roach, J. A. (2014). Chapter 15. Military Cables. Dans D. R. Burnett, R. Beckman et T. M. Davenport (dir.), *Submarine Cables - The Handbook of Law and Policy* (p. 339-349). Brill. <https://doi.org/10.1163/9789004260337_017>, p. 340-341.

stratégique augmente.[37] De nombreux auteurs, tels que Namor, Clark et Annathurai, mettent en lumière ce risque croissant. Namor explique que l'information joue un rôle central dans la conduite des opérations militaires, de la politique et de l'économie. Les routes de transmission d'informations, comme les câbles sous-marins, se retrouvent donc au cœur des enjeux stratégiques, tactiques et géopolitiques.[38] Clark affirme que l'habileté à menacer et à protéger les câbles sous-marins, ainsi que leurs installations côtières, sera de plus en plus importante dans les conflits à venir. En effet, de multiples attaques coordonnées contre le réseau câblé d'un adversaire pourraient interrompre la communication entre les forces armées et les commandants nationaux, tout en limitant considérablement le partage de renseignements militaires. Un contrôle et une surveillance limités des armes stratégiques et des systèmes d'alerte précoce peuvent déstabiliser l'adversaire et ainsi donner un avantage à l'autre partie.[39] Cependant, de telles attaques peuvent entraîner d'importantes conséquences humanitaires pour les populations civiles et les États neutres au conflit qui dépendent des câbles pour leurs communications de base et leur commerce.[40] La perturbation d'une infrastructure civile critique peut ainsi entraîner une instabilité sociale et dégénérer en crise menaçant la sécurité nationale[41], le tout étant aggravé par l'interdépendance intersectorielle.

Les câbles sous-marins à fibre optique sont essentiels pour les télécommunications, tandis que ceux utilisés à des fins militaires, détenus ou loués par l'armée, sont essentiels à la défense et à la sécurité nationales.[42] Les câbles sont donc également considérés comme des infrastructures stratégiques, car ils sont des instruments au service d'une stratégie nationale, ainsi que des outils essentiels à la conduite d'actions visant des objectifs politiques.[43] En résumé, les préoccupations politiques et stratégiques concernant les câbles sous-marins sont les suivantes : les câbles sont des infrastructures critiques qui nécessitent une protection contre les dommages accidentels et les interférences ; les câbles soutiennent la collecte de renseignements dans le domaine maritime ; et les câbles peuvent être affectés lors de batailles navales, que ce soit intentionnellement ou

[37] Annathurai, R. M., *Op. cit.*, p. 4.
[38] Namor, A. (2022). La conquête des routes numériques. *Inflexions, 49*(1), 95-102. <https://doi.org/10.3917/infle.049.0095>, p. 96.
[39] Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists, 72*(4), 234-237. <https://doi.org/10.1080/00963402.2016.1195636>, p. 235.
[40] Annathurai, R. M., *Op. cit.*, p. 4.
[41] Morel, C. (2018), *Op. cit.*, p. 426.
[42] Roach, J. A., *Op. cit.*, p. 349.
[43] Morel, C. (2019), *Op. cit.*, p. 41.

accidentellement.[44] Par ailleurs, les câbles étant des infrastructures au service d'une stratégie nationale, ils reflètent les dynamiques de pouvoir entre États. Le contrôle des modes de communication correspond à un certain contrôle, ou du moins à une influence, sur les autres acteurs étatiques.[45]

Les câbles sous-marins de télécommunications sont des infrastructures critiques et stratégiques caractérisées par l'interdépendance intersectorielle, ce qui illustre l'importance de les protéger. Toutefois, il existe un manque de protection à l'égard des infrastructures physiques qui soutiennent le cyberespace et les technologies de l'information et de la communication (TIC). Ce manque de sécurisation est également observable dans le cas du réseau câblé sous-marin.[46] La prochaine sous-section explore les divers risques et vulnérabilités liés aux câbles et définit le concept de redondance du réseau.

1.2 Vulnérabilités, risques et menaces

Afin de mieux saisir le sujet, il est important de noter que les bris de câbles sous-marins sont des phénomènes très courants. Chaque semaine, deux à quatre câbles sont endommagés dans le monde. Afin d'assurer le maintien des services de télécommunications, les opérateurs répartissent la capacité de leurs réseaux sur plusieurs câbles. C'est ce qu'on appelle la redondance du réseau (*network redundancy*). Ainsi, en cas de rupture d'un câble, le réseau continue de fonctionner sans problème en passant par les autres câbles jusqu'à ce que la détérioration ou la défaillance soit réparée.[47] La redondance renforce donc la résilience des réseaux de communication.[48] Pour réellement nuire au réseau mondial de câbles sous-marins de télécommunications, une attaque majeure est nécessaire et celle-ci doit comprendre de multiples atteintes coordonnées et simultanées. Ce scénario est d'ailleurs peu probable, notamment en raison de la difficulté d'accès à ces infrastructures.[49] Si le concept d'interdépendance intersectorielle exprime la vulnérabilité des

[44] McGeachy, H., *Op. cit.*, p. 169.
[45] Starosielski, N. (2015). Circuitous Routes: From Topology to Topography. Dans *The Undersea Network* (1ère éd., p. 26-63). Durham, États-Unis: Duke University Press. <http://ebookcentral.proquest.com/lib/uqam/detail.action?docID=1974178>, p. 34.
[46] Morel, C. (2016), *Op. cit.*, p. 36.
[47] Burdette, L., *Op. cit.*
[48] Clark, B., *Op. cit.*, p. 235.
[49] Morel, C. (2019), *Op. cit.*, p. 42.

infrastructures critiques, la notion de redondance offre une certaine protection du réseau câblé en garantissant les télécommunications en cas de dommage porté à un câble sous-marin.

Les câbles sous-marins sont tout de même exposés à plusieurs menaces, telles que les risques accidentels et environnementaux, les goulots d'étranglement vulnérables, le sabotage intentionnel de la part d'acteurs étatiques ou non étatiques, ainsi que l'espionnage et d'autres cybermenaces.[50] De manière générale, deux types de vulnérabilités envers ces infrastructures sont identifiés, soit les menaces physiques et cyber.[51] En outre, les pannes de câble ordinaires peuvent ressembler à des actes de sabotage – définis comme des actes intentionnels, illégaux et souvent secrets et clandestins[52] – si les opérateurs ou les gouvernements ne sont pas certains de leur origine. Ceci est un élément clé qui caractérise les moyens d'attaque modernes de la zone grise.[53] Ce concept sera défini dans la revue de la littérature.

Les phénomènes naturels, tels que les éruptions volcaniques, les séismes et les cyclones, sont la cause de 10 % des dommages causés aux câbles sous-marins chaque année. Plus de 60 % des dommages causés au réseau de câbles sont dus aux activités de pêche et de navigation, principalement des coupures par filets de pêche et par le passage d'ancres.[54] Il est estimé que 21 % des dommages subis par les câbles sous-marins ne sont pas identifiés, c'est-à-dire que leur cause n'est pas connue. De nombreuses études excluent les actes volontaires, criminels ou intentionnels, même si ceux-ci sont mentionnés dans les médias. Le dernier pourcentage ci-dessus inclut donc les actes volontaires, même si la part exacte que représentent les atteintes intentionnelles n'est toujours pas connue.[55]

Dans certains endroits, des contraintes géographiques ou réglementaires obligent les câbles à emprunter des corridors étroits, ce qui accroît considérablement le risque de rupture simultanée de plusieurs câbles.[56] Par exemple, le détroit de Malacca est une zone à haute intensité de navigation

[50] Beyer, J. L. *et al*., *Op. cit.*, p. 1.
[51] Morel, C. (2016), *Op. cit.*, p. 37.
[52] Morel, C. (2019), *Op. cit.*, p. 40.
[53] Burdette, L., *Op. cit.*
[54] Morel, C. (2023), *Op. cit.*, p. 83.
[55] Morel, C. (2019), *Op. cit.*, p. 36.
[56] Burdette, L., *Op. cit.*

ainsi qu'un lieu où la détérioration des câbles est plus fréquente. Cette zone contient plus d'une douzaine de câbles qui garantissent la majorité du transit de données entre l'Asie, le Moyen-Orient et l'Europe.[57] Le détroit de Luçon, entre Taïwan et les Philippines, est un autre exemple de goulot d'étranglement, en plus d'être une région particulièrement exposée aux tremblements de terre.[58] Les contraintes géographiques, politiques ou territoriales dans ces zones limitent les itinéraires câblés potentiels.[59] Morel fait remarquer que les « autoroutes de l'information » coïncident bien souvent avec les routes maritimes empruntées par les navires. Cette superposition des routes augmente les risques pour les câbles sous-marins.[60] Pour bien comprendre le sujet des câbles sous-marins, il faut également traiter des stations d'atterrissage, c'est-à-dire les points où les câbles sous-marins atteignent la terre ferme.[61] Le manque de diversité physique du réseau présente un risque pour les infrastructures sous-marines. La tendance à utiliser les mêmes corridors géographiques pour les câbles sous-marins, puis à les faire converger vers les mêmes points d'atterrissage, augmente le risque de dommages simultanés.[62] Une attaque visant une station d'atterrissage engendrerait de nombreux dégâts, car ces sites réunissent en leur sein de nombreux câbles qui permettent le trafic international de données. Ces stations sont donc particulièrement vulnérables.[63]

À cela s'ajoutent les actes de piraterie ou de vandalisme envers ces infrastructures, ainsi que les vols à main armée commis contre les navires câbliers. Ces activités illicites peuvent ralentir le travail des navires câbliers ou mener au vol de composants de câbles[64], comme ce fut le cas en 2007 lorsque des pêcheurs vietnamiens ont volé plus de 500 kilomètres de câbles afin de revendre les matériaux les composant. En raison de cet incident, le Vietnam avait perdu plus de 80 % de sa connectivité mondiale.[65] Un autre exemple de piraterie est celui survenu, encore une fois, au Vietnam en 2017, où les câbles ainsi que les navires qui s'occupent de la pose et de l'entretien des

[57] Brake, D., *Op. cit.*, p. 2.
[58] Morel, C. (2019), *Op. cit.*, p. 42.
[59] Brake, D., *Op. cit.*, p. 2.
[60] Morel, C. (2017), *Op. cit.*, p. 25.
[61] Ross, M. (2014). Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security. *SAIS Review of International Affairs, 34*(1), 141-155. <https://muse.jhu.edu/pub/1/article/547670>, p. 141.
[62] *Ibid.*, p. 143.
[63] Morel, C. (2016), *Op. cit.*, p. 39.
[64] Morel, C. (2023), *Op. cit.*, p. 83-84.
[65] Morel, C. (2016), *Op. cit.*, p. 40.

câbles ont été visés.[66] Par ailleurs, le réseau mondial de câbles sous-marins de télécommunications est largement dominé par les États-Unis, faisant de cette infrastructure un support de l'idéologie occidentale et libérale. Cet aspect fait des câbles sous-marins une cible pertinente pour tout acteur souhaitant nuire à l'ordre international actuel.[67] Effectivement, les groupes terroristes pourraient s'en prendre aux réseaux de câbles. De petites actions, comme des coupures visées, peuvent avoir un impact majeur en déstabilisant les sociétés et leur économie, mais également leurs valeurs et leur organisation.[68]

Concernant la menace d'espionnage, celle-ci se manifeste par le captage direct d'informations, soit une technique de renseignement par câbles sous-marins qui permet l'accès continu à une information massive.[69] Ce risque existe toujours aujourd'hui, comme l'a exposé l'affaire Snowden en 2013 en révélant que les gouvernements américains et britanniques récoltaient des renseignements et des données grâce aux câbles sous-marins et par l'intermédiaire, entre autres, des programmes *Upstream* et *Tempora*.[70] En plus de l'espionnage, des campagnes de censure peuvent être menées, nuisant également à la confidentialité et à la continuité du trafic. La censure consiste à intercepter des informations afin qu'elles n'atteignent pas leur destination. Pendant la guerre froide, les États-Unis ont utilisé des hydrophones nommés « *Sound Surveillance System* » (SOSUS) afin de détecter des sous-marins étrangers à partir du réseau de câbles. Ceci représente une campagne de renseignement ayant mobilisé les câbles sous-marins de manière indirecte.[71] La coupure volontaire d'une liaison sous-marine, l'endommagement d'un site d'atterrissage ou encore la captation d'informations par câble sous-marin sont des actes qui peuvent s'inscrire dans la guerre informationnelle.[72]

D'ailleurs, les circuits de fréquences radio utilisés par les satellites de communication ne disposent pas d'une capacité de réception suffisante pour prendre en charge les téraoctets de données

[66] Morel, C. (2019), *Op. cit.*, p. 37.
[67] *Ibid.*, p. 40.
[68] *Ibid.*, p. 41.
[69] Morel, C. (2015), *Op. cit.*, p. 118.
[70] Morel, C. (2019), *Op. cit.*, p. 39.; Morel, C. (2017), *Op. cit.*, p. 19.
[71] Morel, C. (2019), *Op. cit.*, p. 37.
[72] Morel, C. (2018), *Op. cit.*, p. 426.

enregistrées par les divers appareils.[73] En effet, malgré les avancées technologiques au niveau des satellites, ceux-ci ne sont pas du tout la principale source de connexion Internet. Les câbles sous-marins restent le moyen le plus rapide, le plus efficace et le moins dispendieux de transmettre de l'information d'un point du globe à un autre.[74] Les satellites ne permettent pas d'exécuter tous les ordres opérationnels nécessaires au soutien d'opérations militaires à l'échelle mondiale. C'est la raison pour laquelle les communications militaires classifiées utilisent le même réseau de câbles sous-marins que les données civiles et non confidentielles, ce qui les rend vulnérables aux écoutes et à l'espionnage.[75] Cette infrastructure technologique à double usage fait en sorte que les frontières deviennent de plus en plus floues entre les domaines civil et militaire. En d'autres mots, une infrastructure civile est utilisée à des fins militaires, ce qui constitue une caractéristique des méthodes en zone grise. Ce concept est traité dans la prochaine section.

En plus de décrire les divers risques liés aux câbles sous-marins, cette section a défini les concepts d'infrastructures critiques et stratégiques, d'interdépendance intersectorielle et de redondance du réseau. Ces notions sont nécessaires à la bonne compréhension du sujet et permettent de poursuivre avec les aspects plus théoriques de la revue de la littérature scientifique. Ensemble, ces concepts permettent d'analyser le cas taïwanais.

[73] Clark, B., *Op. cit.*, p. 235.
[74] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 391.
[75] Clark, B., *Op. cit.*, p. 235.

2- REVUE DE LA LITTÉRATURE

La revue de la littérature scientifique permet de mieux saisir l'enjeu géopolitique entourant les systèmes de câbles sous-marins de télécommunications, tout en expliquant le manque d'attention académique portée à ce sujet pourtant primordial. Afin de faciliter la compréhension, la structure de la revue de la littérature est organisée par thèmes, soit l'invisibilité des câbles, la concurrence numérique et les rapports de force, la sécurisation et, finalement, la zone grise. Ces concepts constituent le cadre théorique qui sera utilisé pour analyser le cas de Taïwan.

2.1 L'invisibilité des câbles sous-marins

Malgré leur reconnaissance comme infrastructures critiques et stratégiques, les câbles sous-marins bénéficient d'une attention académique limitée dans les domaines de la sécurité et de la science politique. Bueger et Liebetrau expliquent ce manque d'attention par la « triple invisibilité » des câbles sous-marins, que ce soit en tant qu'infrastructure, dans le sol ou encore dans la mer.[76] Les infrastructures telles que les routes, les ponts, les égouts ou les bâtiments ont tendance à être prises pour acquises, invisibles et oubliées en raison de leur intégration à la vie quotidienne, faisant ainsi partie du paysage. Dans le cas des câbles sous-marins, ceux-ci sont encore plus invisibles puisqu'ils se trouvent sous le sol. En effet, ils ne sont pas visibles au quotidien et leur réparation ne cause généralement pas de rupture de service (notamment en raison de la redondance du réseau), attirant ainsi très peu d'attention à leur égard. Ils font donc partie des infrastructures les moins visibles. Enfin, les câbles se trouvent sous la surface, en haute mer. Dans les discours de politique internationale, les mers et les océans sont souvent traités comme des espaces lointains où les activités humaines sont limitées, ou bien comme des espaces qui ne nécessitent pas de règles et de réglementations autres que celles établies par la Convention des Nations unies sur le droit de la mer (UNCLOS – United Nations Convention on the Law of the Sea). Ce phénomène est nommé « *sea blindness* ». L'étude de la sécurité maritime et l'attention portée aux vulnérabilités en haute mer n'ont pris de l'ampleur que ces dernières années.[77] De manière similaire, Fernandes considère les câbles sous-marins de télécommunications, les opérations sous-marines et les opérations d'espionnage comme des sphères invisibles aux yeux du public en raison de leur caractère

[76] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 392.
[77] *Ibid.*, p. 393-394.

souterrain.[78] En plus de ces formes d'invisibilité, Morel soutient que la difficulté d'accès à ces infrastructures et leur caractère confidentiel expliquent en partie le manque d'études scientifiques sur le sujet, ce qui renforce d'ailleurs leur invisibilité académique.[79] Alors que les câbles sous-marins sont des infrastructures enterrées, immergées et donc invisibles, les recherches scientifiques à leur sujet adoptent en outre des approches limitées.

Bueger et Liebetrau démontrent que la communauté scientifique s'est penchée sur le sujet des câbles sous-marins selon trois approches principales. Or, le manque de diversité quant aux approches adoptées participe à l'invisibilité de ces infrastructures, ou du moins limite leur compréhension. Il y a d'abord l'étude du sujet selon un discours sécuritaire, c'est-à-dire la protection des câbles contre les dangers comme la guerre hybride et les attaques terroristes. Autrement dit, cette approche traite des risques et des menaces intentionnels auxquels font face les câbles sous-marins. Ensuite, il y a l'étude du sujet selon un point de vue technique, c'est-à-dire les risques habituels et les dommages de routine que subissent les câbles, ainsi que les manières d'y remédier et de les réparer. Cette approche traite donc des risques et des menaces non intentionnels auxquels sont confrontés les câbles à fibre optique. Enfin, il y a l'étude juridique du sujet, plus précisément concernant les systèmes internationaux actuels qui permettent de réguler et de réglementer les enjeux relatifs aux câbles sous-marins. Comme le soulignent Burger et Liebetrau, ces trois approches sont restrictives, car elles ne prennent pas suffisamment en compte les questions politiques et stratégiques qui touchent le réseau de câbles.[80] McGeachy résume bien cette lacune en affirmant que les recherches académiques se restreignent traditionnellement à la protection des câbles contre les menaces externes.[81] Certains auteurs suggèrent, par exemple, l'usage des véhicules sous-marins sans pilote (UUVs – Unmanned Undersea Vehicles) afin de protéger les câbles contre d'éventuels incidents, attaques ou autres menaces.[82] Ces approches limitées dans l'étude des câbles sous-marins contribuent donc à leur invisibilité, tout en révélant le manque de recherche sur les aspects politiques et stratégiques vis-à-vis des câbles.

---

[78] Fernandes, C. (2021). Subterranean statecraft: Invisible diplomacy in Australia's external relations. *Geoforum, 127*, 385-389. <https://doi.org/10.1016/j.geoforum.2020.02.007>, p. 385.
[79] Morel, C. (2019), *Op. cit.*, p. 34-35.
[80] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 392.
[81] McGeachy, H., *Op. cit.*, p. 161-162.
[82] Clark, B., *Op. cit.*, p. 235-236; Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). *Marine Policy, 171*(106434). <https://doi.org/10.1016/j.marpol.2024.106434>.

D'ailleurs, les infrastructures sous-marines ne sont pas signalées publiquement, ce qui rend leur identification difficile. La localisation exacte des câbles est toutefois partagée aux pêcheurs et autres acteurs maritimes afin qu'ils évitent ces zones sensibles. Si les cartes nautiques ne sont pas rendues publiques, l'accès à l'information en sources ouvertes et aux nouvelles technologies comme les UUVs facilitent l'identification et l'atteinte des câbles. Ceci constitue un risque émergent. Morel ajoute que les câbles sous-marins ont autrefois bénéficié de leur discrétion et de leur invisibilité, ces facteurs ayant contribué à leur protection. Cependant, cette invisibilité contribue aujourd'hui à la méconnaissance du sujet et au manque de réaction d'urgence en cas de crise.[83]

Les câbles sous-marins étant caractérisés par les diverses formes d'invisibilité susmentionnées, il est compréhensible que ces infrastructures soient plus difficilement étudiées et que les approches de recherche soient limitées. Ces lacunes deviennent particulièrement apparentes lorsque des incidents visant ces câbles surviennent, comme c'est le cas à Taïwan, car elles entraînent une méconnaissance du sujet. Autrement dit, les câbles sont caractérisés par diverses formes d'invisibilité, ce qui se traduit également par une carence d'études sur le sujet dans la littérature en études stratégiques et en science politique. Afin de mieux saisir le sujet, la sous-section suivante traite des principaux acteurs impliqués dans les réseaux de câbles dans le contexte de la concurrence numérique.

2.2 Les acteurs, la concurrence numérique et les rapports de force

Cette sous-section traite d'abord des acteurs privés et étatiques, éléments essentiels pour ensuite aborder la concurrence numérique. Par la suite, la place structurelle des États dans le réseau mondial de câbles sous-marins est abordée, ce qui permet de mettre en lumière les dynamiques de pouvoir dans ce domaine. Les rapports de force dans le domaine câblé s'appliquent également au cas de Taïwan, ce qui souligne l'importance d'aborder ce sujet.

[83] Morel, C. (2018), *Op. cit.*, p. 423-424.

Le caractère interdépendant est inhérent aux réseaux de câbles sous-marins pour plusieurs raisons. Tout d'abord, les itinéraires de câbles appartiennent à des consortiums d'entreprises qui se partagent leur propriété, ce qui signifie qu'aucun acteur ne possède l'entièreté du réseau à lui seul. Ensuite, les câbles sont soumis à la juridiction nationale et internationale, ce qui implique que les entreprises et les États doivent collaborer pour réparer les câbles endommagés ou poser de nouveaux câbles. Enfin, le réseau mondial de câbles est également considéré comme interdépendant en raison de l'interconnexion qu'il crée en reliant les différents acteurs entre eux.[84] L'augmentation du nombre d'acteurs du secteur privé complexifie l'étude des câbles sous-marins, car ces acteurs sont multiples, peu connus et leurs actions sont souvent interconnectées.[85] Morel décrit trois types d'acteurs privés dans le domaine câblé. Premièrement, les acteurs clés du secteur sont les fournisseurs de systèmes sous-marins, c'est-à-dire les fabricants de câbles. Deuxièmement, il y a les propriétaires de câbles, qui se regroupent bien souvent en consortium d'opérateurs. Troisièmement, les armateurs s'occupent de poser les câbles et de les réparer. Quant aux États, ils agissent également dans le secteur câblé par le biais de leurs entreprises nationales ou publiques, c'est-à-dire les entreprises possédées ou soutenues par l'État.[86] Fernandes établit le lien entre les acteurs privés et étatiques. L'auteur défend l'idée selon laquelle l'étude des domaines souterrains et invisibles, tels que les câbles sous-marins, révèle certaines dimensions cachées de la politique d'un État, notamment l'influence du secteur privé sur les intérêts nationaux et les objectifs de sécurité nationale. Concernant la notion d'intérêt national, l'auteur s'éloigne de la définition traditionnelle des réalistes en relations internationales. Alors que les réalistes considèrent la défense et la sécurité comme des éléments fondamentaux de l'intérêt national, Fernandes est plutôt d'avis que le réel intérêt principal est la sécurité du pouvoir étatique face au public national, composé essentiellement de la société civile et du secteur privé. Autrement dit, les politiques gouvernementales se préoccupent des intérêts des principaux groupes d'intérêt nationaux, en particulier les entreprises privées.[87] Si le secteur privé exerce une influence sur les intérêts nationaux, d'autres auteurs montrent aussi le phénomène inverse, comme quoi les États détiennent une certaine marge de manœuvre à travers leurs entreprises nationales. Winseck observe, quant à lui, deux tendances majeures en Indo-Pacifique, tout en précisant que l'économie géopolitique

[84] Ross, M., *Op. cit.*, p. 143.
[85] Morel, C. (2019), *Op. cit.*, p. 34-35.
[86] *Ibid.*, p. 35-36.
[87] Fernandes, C., *Op. cit.*, p. 385.

d'Internet a pivoté vers cette région. Tout d'abord, les entreprises publiques ou nationales jouent un rôle plus actif dans les consortiums de câbles de cette région. Ensuite, l'auteur soutient que la Chine est devenue un acteur important dans le domaine câblé. Selon lui, les gouvernements deviennent donc plus actifs en ce qui concerne les enjeux d'infrastructures d'Internet dans la région indo-pacifique.[88] En d'autres termes, les gouvernements sont davantage actifs dans le domaine câblé par le biais des entreprises publiques et/ou des entreprises privées, ce qui suggère une influence mutuelle entre les secteurs public et privé. Winseck vient donc nuancer les propos de Fernandes tout en soutenant l'analyse de Morel. Tel que susmentionné, même si ce travail reconnaît et tient compte de l'influence mutuelle entre les secteurs privé et public, l'étude se concentre plutôt sur les acteurs étatiques et, notamment, sur la compétition numérique caractérisée par la zone grise.

Depuis quelques années, l'étude des câbles sous-marins selon l'approche sécuritaire inclut également la concurrence entre grandes puissances.[89] Alors que les câbles sous-marins étaient autrefois traités comme un service public relevant des entreprises privées, ils sont maintenant reconnus comme un sujet de compétition technologique stratégique entre les grandes puissances mondiales, notamment les États-Unis et la Chine, qui s'affrontent dans une course à la supériorité technologique. Alors que le rôle des acteurs étatiques dans les enjeux liés aux câbles est bien reconnu, McGeachy montre que la compétition technologique stratégique a modifié la perception des câbles sous-marins, qui sont désormais perçus non seulement comme des infrastructures critiques devant être protégées contre des menaces extérieures, mais également comme des vecteurs d'influence et de menace.[90] Autrement dit, au lieu de se concentrer presque exclusivement sur la protection des câbles, comme c'était le cas auparavant, le réseau de câbles sous-marins est désormais considéré comme une menace en soi, dépendamment de qui le possède, le construit et le contrôle. Cette évolution marque un changement dans l'étude du sujet par la communauté scientifique. Plus précisément, la concurrence numérique stratégique est devenue un argument majeur pour justifier l'engagement des États-Unis et de leurs alliés dans le secteur des câbles sous-marins. McGeachy conclut que, malgré son importance stratégique croissante dans le contexte de

[88] Winseck, D. (2017). The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy, 7*, 228-267. <https://doi.org/10.5325/jinfopoli.7.2017.0228>, p. 256.
[89] Noor, E. (2024). Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables?lang=en>.
[90] McGeachy, H., *Op. cit.*, p. 162.

la rivalité sino-américaine pour le leadership en matière de capacités technologiques, le secteur des câbles ne reflète pas, et ne reflétera probablement jamais, de manière directe les intérêts nationaux puisqu'il est difficile d'exercer une influence dans ce domaine.[91] Cette conclusion montre un certain désaccord au sein de la communauté scientifique, notamment par rapport aux travaux de Fernandes (le secteur privé influence les intérêts nationaux) et de Winseck (les États assurent leurs intérêts nationaux à travers leurs entreprises publiques). Ainsi, les câbles sous-marins occupent une part limitée, mais pertinente, de la compétition technologique. Les recherches qui se concentrent sur les États en tant qu'acteurs principaux du réseau câblé étudient principalement le sujet sous l'angle de la concurrence numérique ou de la compétition technologique stratégique.

D'ailleurs, les acteurs et la concurrence numérique reflètent les rapports de force au sein du réseau câblé. En s'appuyant sur les travaux de Carr[92], McGeachy explique que la gouvernance et les infrastructures d'Internet renforcent les dynamiques de pouvoir déjà existantes.[93] Ross, quant à elle, nomme une caractéristique particulière du réseau de câbles par le terme « *betweenness centrality* ». Ce terme indique à quel point un acteur se trouve sur le chemin le plus court entre d'autres paires d'acteurs du réseau. Plus un État se situe au centre de cette interconnexion, plus il est susceptible d'avoir un nombre élevé de sites d'atterrissage de câbles sous-marins.[94] Singapour et la Malaisie présentent tous deux cette caractéristique particulière du fait de leur position géographique qui coïncide avec le détroit de Malacca et qui exprime leur centralité structurelle dans le réseau câblé. Ross ajoute que les États ayant une forte interconnexion (*high-betweenness*) sont structurellement importants pour le fonctionnement de l'ensemble du réseau. Ainsi, un dommage majeur subi par les câbles d'un État à forte interconnexion aura un impact plus important sur les autres États du réseau, comparé à un dommage similaire survenant dans un État à faible interconnexion.[95] Ceci reflète non seulement les enjeux sécuritaires relatifs aux câbles sous-marins, mais également les rapports de force entre États dans le domaine câblé. Les États-Unis sont le pays présentant la plus forte interconnexion du réseau et le plus grand nombre de sites d'atterrissage. En effet, les États-Unis relient les pays d'Amérique du Sud aux pays d'Asie de l'Est, ceux-ci n'étant

[91] *Ibid.*, p. 173.
[92] Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium, 43*(2), 640-659. <https://doi.org/10.1177/0305829814562655>.
[93] McGeachy, H., *Op. cit.*, p. 164.
[94] Ross, M., *Op. cit.*, p. 145.
[95] *Ibid.*, p. 148.

pas directement connectés par le réseau mondial de câbles. Par ailleurs, les États qui occupent une position géographique à forte interconnexion, mais qui ne possèdent pas un nombre élevé de points d'atterrissage, créent des goulots d'étranglement qui présentent un risque potentiel pour l'ensemble du réseau.[96] La position structurelle des États dans le réseau de câbles sous-marins exprime donc en partie les rapports de force dans le domaine câblé, ce qui est particulièrement pertinent dans l'analyse du cas taïwanais, où la rivalité sino-américaine et les opérations en zone grise sont présentes.

Maintenant que les rapports de force, la concurrence numérique et les divers acteurs ont été abordés, il est nécessaire de définir le concept de sécurisation. Ce concept permet de comprendre les réactions des États face aux enjeux relatifs aux câbles sous-marins. Comme mentionné précédemment, même si Taïwan n'est pas reconnu comme un État souverain sur la scène internationale, le concept de sécurisation s'applique à son cas en raison de son statut particulier qui lui apporte une certaine indépendance décisionnelle.

2.3 La sécurisation des câbles et l'enjeu de classification

La sécurité consiste à se libérer de toute menace, tandis que la « sécurisation » d'un enjeu renvoie au processus permettant de le rendre exempt de toute menace. La sécurisation d'un enjeu, dans ce cas-ci celui du réseau interdépendant de câbles, est un processus particulier qui nécessite deux facteurs. Tout d'abord, un acteur malveillant doit être identifié comme représentant une menace existentielle à l'égard du réseau de câbles sous-marins, révélant ainsi la nécessité de protéger ces infrastructures critiques. L'acteur malveillant peut être un État, un groupe terroriste ou encore d'autres acteurs négligents. Ensuite, les parties prenantes de l'infrastructure de câbles, c'est-à-dire les entreprises, les gouvernements et la société civile, doivent être convaincues de la nécessité de protéger le réseau, ce qui justifie l'adoption de mesures particulières pour le sécuriser. Cependant, la sécurisation des câbles sous-marins révèle de nombreuses contradictions, le concept de sécurité étant controversé et intersubjectif. En effet, les États ne partagent pas les mêmes perceptions de sécurité ou d'insécurité, ce qui complique la sécurisation des infrastructures sous-marines

[96] *Ibid.*, p. 149.

internationales et interdépendantes.[97] Ross ne démontre pas que les États adoptent des méthodes de sécurisation différentes à l'égard de l'infrastructure de câbles. Toutefois, l'autrice apporte une contribution pertinente en montrant que le réseau mondial de câbles devient de plus en plus interdépendant, ce qui signifie qu'il est plus difficile pour un acteur de nuire intentionnellement aux télécommunications d'un autre acteur sans nuire aux siennes. Ceci renvoie aux concepts d'interdépendance et de redondance des réseaux, ou de *network redundancy* en anglais. Les caractéristiques structurelles du réseau montrent cependant que tous les États ne sont pas égaux face à ce genre de menace et à ses conséquences.[98] Morel se montre en accord avec Ross en tenant les propos suivants : « En théorie, l'interdépendance des flux qui domine aujourd'hui au niveau mondial laisse supposer qu'en effet, les États ne peuvent plus perturber la continuité des communications internationales sans en subir eux-mêmes les conséquences. »[99] De plus, Morel donne plusieurs exemples de sécurisation des câbles sous-marins menés à l'initiative des États. S'il n'existe pas d'initiative au niveau international, les États peuvent tout de même agir à leur échelle nationale. Parmi les exemples, il y a les investissements nationaux dans ces infrastructures sous-marines, l'obligation pour les entreprises privées d'obtenir l'autorisation de l'État avant de débuter un projet de câblage, ou encore la présence d'autres infrastructures militaires à proximité des câbles de communication.[100] Quant aux entreprises privées, elles déterminent les itinéraires des câbles notamment en fonction de l'aspect sécuritaire de sorte à prévenir les interférences, qu'il s'agisse de catastrophes naturelles ou de tensions géopolitiques.[101] L'attribution ou la classification d'un incident, c'est-à-dire l'identification de sa cause et de son intention, permet de déterminer une réponse adéquate à l'acte en question et de participer ainsi à un processus de sécurisation. Les concepts de sécurisation et de classification sont donc étroitement liés. Les termes « attribution » et « classification » sont utilisés comme des synonymes dans le présent travail.

Dans l'un de ses articles, Morel vise à classifier les dommages subis par les liaisons sous-marines de télécommunications. L'autrice se penche spécifiquement sur les attaques volontaires, et donc intentionnelles, à l'encontre du réseau de câbles sous-marins. Ainsi, son article vise à caractériser

---

[97] Ross, M., *Op. cit.*, p. 143.; Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Boulder, Colorado: L. Rienner, 2nd ed.
[98] Ross, M., *Op. cit.*, p. 152.
[99] Morel, C. (2019), *Op. cit.*, p. 39.
[100] *Ibid.*
[101] Starosielski, N., *Op. cit.*, p. 29.

les différentes atteintes portées aux réseaux câblés, à évaluer le rôle de l'État comme acteur hostile et opérateur du réseau, ainsi qu'à expliquer les intérêts stratégiques de ces infrastructures critiques sous-marines.[102] Morel étudie la question de la classification selon deux catégories d'analyse, soit l'acteur à l'origine de l'acte et l'acte en lui-même. L'acteur peut être étatique, non étatique ou encore agissant par l'intermédiaire d'individus distincts de l'État. L'acte peut être une action directe sur le réseau physique ou encore une action indirecte visant l'information transitant par le câble.[103] En outre, Morel note une évolution quant aux menaces volontaires à l'encontre des câbles. Si les États belligérants étaient autrefois les principaux acteurs lors de conflits, ce cadre s'est aujourd'hui élargi pour inclure les individus et les moments de paix où il n'y a pas de conflit direct. Les individus agissent soit par eux-mêmes, soit avec le soutien d'un acteur étatique.[104] Avec sa typologie des atteintes volontaires au système sous-marin de télécommunications, Morel apporte une contribution particulièrement pertinente à l'attribution et à la classification des actes visant les câbles. Cette typologie et le concept de sécurisation seront utilisés pour étudier les cas survenus à Taïwan, permettant ainsi de caractériser les atteintes et de décrire les réponses adoptées.

Par ailleurs, Morel explique que presque aucune action directe d'un acteur étatique sur des câbles sous-marins n'a été attribuée depuis la Seconde Guerre mondiale. Elle observe plutôt des actes non étatiques qui seraient potentiellement soutenus par un État, mais qui ne sont pas revendiqués de la sorte.[105] Cette difficulté d'attribution rend la sécurisation plus ardue. Ce flou intentionnel peut s'inscrire dans les actions dites « en zone grise », un concept décrit dans la sous-section suivante.

2.4 La zone grise, une stratégie non-conventionnelle

Un exemple parfait pour illustrer le concept de zone grise est celui d'un navire de pêche qui laisserait traîner son ancre sur les fonds marins afin d'endommager des câbles de communication. L'ancrage est un outil simple et efficace pour un acteur malintentionné qui souhaite agir tout en faisant passer l'acte pour un accident.[106] La « zone grise » désigne les méthodes indirectes employées par des États dans le but d'obtenir un avantage sur leur adversaire, et ce, sans recourir

[102] Morel, C. (2019), *Op. cit.*, p. 36.
[103] *Ibid.*, p. 38.
[104] *Ibid.*, p. 36.
[105] *Ibid.*, p. 39.
[106] *Ibid.*, p. 36.

à la guerre ouverte et à la force cinétique. Les actions en zone grise sont coercitives et visent à entraîner un changement, mais tout en évitant toute réaction potentielle de l'adversaire. Entretenir le flou autour de ces opérations en zone grise permet à l'État agresseur d'éviter toute poursuite ou accusation de la part de l'État visé. Autrement dit, ces opérations sont bien souvent délibérément conçues pour rester sous le seuil du conflit militaire conventionnel, pour ne pas dépasser les lignes rouges établies et pour obtenir des gains, mais sans exposer l'État agresseur aux conséquences qu'une escalade militaire entraînerait. Par ailleurs, la zone grise fait partie de la notion de « guerre hybride ». La guerre hybride fait référence à l'usage simultané de méthodes militaires conventionnelles ainsi que de méthodes secrètes et non conventionnelles, ces dernières pouvant inclure des opérations non cinétiques et en zone grise.[107]

Dans le cas des opérations maritimes en zone grise, Goldrick affirme que celles-ci sont presque toujours reliées à des revendications de souveraineté sur des zones géographiques et maritimes. Les opérations maritimes en zone grise peuvent toutefois avoir d'autres motifs, comme exercer une pression supplémentaire sur l'adversaire afin de le faire plier aux résultats désirés par l'État agresseur, même si ces résultats ne sont pas liés aux revendications maritimes. Selon cette même logique, un État peut recourir à d'autres moyens en zone grise qui sont non maritimes afin d'obtenir des gains territoriaux maritimes.[108] Même si les méthodes en zone grise visent habituellement à éviter toute escalade militaire, il arrive que des États puissants recourent à ces méthodes afin de pousser des États plus faibles à passer à l'action en premier. Cette technique permet ensuite à l'État puissant d'accuser l'État plus faible d'être à l'origine du conflit armé et d'être l'agresseur, tout en étant conscient de sa supériorité militaire et de sa très probable victoire. Goldrick ajoute que les opérations en zone grise n'ont pas à être absolues pour atteindre leur objectif, mais seulement suffisantes. Un effet qui est suffisant remet en question la capacité de contrôle d'un État, le pousse à arrêter d'exploiter économiquement certaines zones maritimes ou encore à interrompre le passage de ses navires dans certaines régions.[109]

---

[107] Goldrick, J. (2018). *Grey Zone Operations and the Maritime Domain* [Special report]. Australian Strategic Policy Institute (ASPI). <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ASPI_SR%20131%20Grey%20zone%20operations.pdf>, p. 4.
[108] *Ibid.*, p. 5.
[109] *Ibid.*, p. 5.

De plus, les opérations en zone grise peuvent être exercées par un État faible envers un État puissant et vice-versa.[110] Goldrick s'appuie sur deux études de cas pour illustrer ces deux dynamiques de pouvoir. Il prend d'abord l'exemple du Royaume-Uni et de l'Islande entre 1958 et 1976. L'Islande, un État faible par rapport au Royaume-Uni, est parvenu à changer petit à petit le statu quo à son avantage en combinant des opérations directes en zone grise, des pressions politiques et la construction d'un narratif qui lui est favorable.[111] L'auteur donne ensuite l'exemple de la Chine et du Vietnam en 1974, la puissance chinoise étant parvenue à obtenir des îles revendiquées par le Vietnam dans l'archipel des Paracels en MCM. La Chine a augmenté graduellement la pression sur le Vietnam tout en utilisant des navires de pêche civils contrôlés par le gouvernement chinois. Dans ce cas-ci, des affrontements militaires directs ont eu lieu, mais la Chine s'est présentée comme la victime forcée de répliquer par légitime défense, alors que le Vietnam a été perçu comme la cause de l'escalade en portant le premier coup.[112] Aujourd'hui encore, la Chine est considérée comme un acteur qui utilise fréquemment des stratégies maritimes en zone grise, que ce soit dans sa zone économique exclusive (ZEE) revendiquée ou encore dans les territoires qu'elle revendique en MCM.[113] L'utilisation de navires de pêche civils illustre la manière dont les frontières entre les domaines civil et militaire deviennent poreuses dans des situations en zone grise. C'est également un exemple de la manière dont il est possible de maintenir un flou et une confusion quant à l'intention d'un acteur étatique.

Concernant les câbles sous-marins de fibre optique, l'auteur prévient que leur perturbation ou leur interférence peut devenir un outil de la zone grise dans le cas de confrontations plus intenses, et particulièrement si les câbles constituent la principale source de communication de territoires extracôtiers isolés.[114] Encore une fois, les frontières entre les domaines civil et militaire deviennent poreuses, avec des conséquences qui affectent non seulement l'État visé et ses forces armées, mais également la population civile. Ces infrastructures d'Internet sont utilisées à des fins civiles, mais aussi pour servir des objectifs politiques et stratégiques s'inscrivant dans la zone grise. Enfin, il est important de souligner le rôle majeur joué par la gestion de l'information et des narratifs dans les

[110] *Ibid.*
[111] *Ibid.*, p. 8-9.
[112] *Ibid.*, p. 9-10.
[113] *Ibid.*, p. 15.
[114] *Ibid.*, p. 25.

opérations en zone grise. Contrôler le narratif permet d'étiqueter l'adversaire comme étant l'agresseur, même si ses actions résultent de provocations en zone grise.[115]

Ainsi, la zone grise caractérise de plus en plus les conflits contemporains, ceux-ci étant de plus en plus indirects et restant sous le seuil de la guerre ouverte. Les tensions entre la Chine et Taïwan sont également caractérisées par les méthodes en zone grise. Les coupures de câbles sous-marins survenues à Taïwan en 2023 et 2025 expriment une tendance croissante quant à l'instrumentalisation de ces infrastructures par la Chine pour exercer une pression supplémentaire sur Taïwan.

Malgré leurs multiples formes d'invisibilité, les câbles sous-marins se retrouvent parmi les technologies qui caractérisent la concurrence numérique sino-américaine en Asie du Sud-Est et en MCM. Leur sécurisation est complexe en raison de l'interconnexion multinationale des réseaux, qui implique de nombreux acteurs étatiques et privés, ainsi que plusieurs législations. La classification des dommages potentiellement intentionnels subis par les câbles reste ardue, notamment en raison des méthodes en zone grise. Ces concepts sont nécessaires pour étudier le cas de Taïwan et de la Chine. La prochaine section se concentre sur les dommages intentionnels en Asie du Sud-Est et en MCM, et plus particulièrement à Taïwan. Les réactions et les stratégies de sécurisation en réponse aux incidents volontaires sont également abordées.

[115] *Ibid.*, p. 9.

3- LES STRATÉGIES DE SÉCURISATION ET LE CAS TAÏWANAIS

Comme expliqué précédemment, les câbles sous-marins sont des infrastructures stratégiques, car ils servent une stratégie nationale et des objectifs politiques.[116] De nombreux États sont conscients de la nécessité de sécuriser ces infrastructures sous-marines de télécommunications, la supériorité technologique et le contrôle de l'information constituant des intérêts stratégiques. Cette section vise donc à déterminer les différentes stratégies adoptées par les États concernés par les enjeux entourant ces câbles. Une cartographie des câbles sous-marins dans la région permet d'abord d'illustrer l'état des lieux et les dynamiques de pouvoir inhérentes au réseau câblé. Après quoi, les divers cas intentionnels survenus dans la région sont présentés. Une attention particulière est portée aux cas taïwanais, ceux-ci étant récents et comportant de sérieux soupçons envers un acteur étatique, c'est-à-dire la Chine. L'exemple de Taïwan révèle une continuité de la compétition technologique stratégique entre les États-Unis et la Chine, ainsi que l'émergence de techniques en zone grise visant les câbles sous-marins. Le cas de Taïwan montre également que les câbles sont désormais considérés comme des vecteurs d'influence et de menace, et non plus seulement comme des infrastructures critiques à protéger contre les menaces extérieures. La concurrence numérique sino-américaine et les stratégies de sécurisation font l'objet de la dernière sous-section.

3.1 La cartographie des câbles en Asie du Sud-Est et à Taïwan

Il est important de cartographier le réseau câblé en Asie du Sud-Est et en MCM afin d'illustrer la position structurelle des États et les dynamiques de pouvoir en lien avec ces infrastructures essentielles. La position structurelle des États au sein de ce réseau permet également de mieux comprendre leurs stratégies de sécurisation. (*Voir la figure 2 en annexe pour une carte des câbles sous-marins dans la région*).

Singapour est l'État membre de l'ASEAN qui est connecté par le plus de câbles sous-marins, avec un total de 25 câbles. Singapour est non seulement considéré comme un territoire stable, mais il se trouve également à l'extrémité du détroit de Malacca, faisant de la Cité-État un lieu privilégié pour les câbles régionaux et internationaux.[117] Après Singapour, la Malaisie est le second pays le plus

[116] Morel, C. (2019), *Op. cit.*, p. 41.
[117] Morel, C. (2023), *Op. cit.*, p. 79-80.

connecté avec 21 câbles sous-marins. Le pays dispose de nombreux points d'arrivée pour les câbles sur chacune de ses façades maritimes. La diversité de points d'atterrissage garantit une plus grande résilience en cas d'endommagement de câbles.[118] Singapour et la Malaisie occupent une position géographique à forte interconnexion (*high-betweenness*), ce qui fait d'eux des acteurs structurellement importants pour le fonctionnement de l'ensemble du réseau.[119]

Ensuite, l'Indonésie possède 42 câbles sous-marins, mais la majorité sert à connecter ses différentes îles de l'archipel entre elles. L'autre partie des câbles sert à connecter, surtout de manière bilatérale, l'Indonésie aux pays avoisinants avec, notamment, sept câbles la reliant à Singapour et six autres à la Malaisie. Ainsi, l'Indonésie possède également une diversité de points d'arrivée de la fibre optique sur son territoire. Quant aux Philippines, elles possèdent seize câbles sous-marins au total, dont six liaisons domestiques, cinq câbles régionaux et cinq câbles internationaux. La Thaïlande compte, quant à elle, huit câbles sous-marins, dont cinq sont d'envergure internationale. D'ailleurs, la Thaïlande offre une alternative au détroit de Malacca, qui concentre déjà de nombreux flux maritimes, en proposant un lien direct entre l'océan Indien et le golfe de Thaïlande par une voie terrestre entre les villes de Satun et de Songkhla.[120]

Le Vietnam ne possède que cinq câbles sous-marins et deux points d'atterrissage. Le Myanmar est desservi par trois câbles vers l'Europe, soit le Southeast Asia - Middle East - Western Europe 3 (SMW3), le Southeast Asia - Middle East - Western Europe 5 (SMW5) et le câble Asia-Africa-Europe-1 (AAE-1). Brunei est également desservi par trois câbles, soit les liaisons Asia-America Gateway (AAG), SMW3 et Southeast Asia-Japan (SJC). Le Cambodge n'est connecté que depuis 2017 et compte aujourd'hui deux câbles, c'est-à-dire la connexion internationale AAE-1 et la liaison régionale Malaysia-Cambodia-Thailand (MCT). Avant 2017, le Cambodge dépendait des liaisons terrestres avec les pays voisins.[121] Le Timor-Leste ne possède qu'un seul câble sous-marin. L'installation de son premier câble sous-marin a débuté en juin 2024 dans le cadre du projet Timor-Leste South Submarine Cable (TLSSC).[122] Ce câble relie Dili, la capitale du Timor-Leste, au câble

[118] *Ibid.*, p. 80-81.
[119] Ross, M., *Op. cit.*, p. 148.
[120] Morel, C. (2023), *Op. cit.*, p. 81.
[121] *Ibid.*, p. 82.
[122] Government of Timor-Leste. (2024, 25 juin). *Government Carries Out First Submarine Fiber Optic Cable Installation*. <https://timor-leste.gov.tl/?p=38073&lang=en&n=1>.

North-West qui a des points d'atterrissage en Australie.[123] Finalement, en tant que pays enclavé, le Laos n'est évidemment pas desservi par des câbles sous-marins, mais plutôt par des liaisons terrestres qui transitent par les pays voisins pour le connecter à l'Internet mondial.[124] En ce qui concerne Taïwan, elle est desservie par quatorze câbles sous-marins internationaux et par dix liaisons nationales, pour un total de 24 câbles.[125]

3.2 Les incidents suspects et la difficulté d'attribution

Cette sous-section décrit les incidents intentionnels survenus en Asie du Sud-Est et en MCM en se basant principalement sur un rapport publié par l'université de Washington qui se penche sur trois études de cas, c'est-à-dire la mer Baltique, la mer de Chine méridionale et la mer Rouge. Ce rapport se concentre principalement sur les actions directes visant le réseau physique de câbles, et non sur les actions indirectes qui visent l'information transitant par ces câbles. Le rapport constate que les conflits liés à l'infrastructure d'Internet reflètent les principaux conflits géopolitiques de chaque région, ainsi que la concurrence entre les États-Unis, la Chine et la Russie. Les États-Unis et la Chine traitent les câbles sous-marins comme une question de sécurité nationale et s'engagent dans une compétition pour le contrôle de cette infrastructure. La Russie, quant à elle, est davantage préoccupée par le développement de capacités offensives pour lancer des attaques contre ces câbles.[126] Ce même rapport recense les incidents majeurs et suspects, c'est-à-dire potentiellement intentionnels, survenus entre 2005 et 2025. Si le rapport fait état de 22 incidents potentiellement intentionnels au total, le présent travail se concentre uniquement sur ceux survenus en Asie du Sud-Est et en MCM. Le rapport a recensé six incidents suspects survenus dans la région entre mars 2007 et février 2025. Parmi ces incidents, trois concernent Taïwan (février 2023, janvier 2025, février 2025), alors que les trois autres concernent respectivement le Vietnam (mars 2007), les

[123] The Australian Infrastructure Financing Facility for the Pacific (AIFFP). (s.d.). *Connecting Timor-Leste to the internet via submarine cable*. <https://www.aiffp.gov.au/investments/investment-list/connecting-timor-leste-to-the-internet-via-submarine-cable>.
[124] Morel, C. (2023), *Op. cit.*, p. 82.
[125] RFI. (2025, 11 avril). Taïwan : un capitaine chinois inculpé pour avoir coupé un câble sous-marin essentiel pour l'île. *RFI (Radio France Internationale)*, Asie-Pacifique. <https://www.rfi.fr/fr/asie-pacifique/20250411-ta%C3%AFwan-un-capitaine-chinois-inculp%C3%A9-pour-avoir-coup%C3%A9-un-c%C3%A2ble-sous-marin-essentiel-pour-l-%C3%AEle>. ; Marine & Océans. (2025, 12 juin). Taïwan : un capitaine chinois emprisonné pour avoir sectionné un câble sous-marin. *Marine & Océans* (Taipei). <https://marine-oceans.com/actualites/taiwan-un-capitaine-chinois-emprisonne-pour-avoir-sectionne-un-cable-sous-marin/>.
[126] Beyer, J. L. *et al*., *Op. cit.*, p. 1.

Philippines (juin 2010) et l'Indonésie (mars 2013).[127] Ces dernières années, l'augmentation des soupçons d'actes de sabotage intentionnels correspond à l'accroissement des tensions géopolitiques, notamment à la suite des attaques contre le gazoduc Nord Stream en 2022 et de l'invasion de l'Ukraine par la Russie. Cela indique que les câbles sous-marins font désormais partie intégrante des menaces hybrides et des opérations en zone grise.[128]

En mars 2007, des pêcheurs locaux ont coupé et volé au moins onze kilomètres de la portion vietnamienne du câble SMW3. Cet incident a eu lieu dans la mer Cà Mau, probablement dans la ZEE du Vietnam. La connexion Internet a été considérablement ralentie et les communications du Vietnam avec Hong Kong et la Thaïlande ont été perturbées pendant près de trois mois. Vietnam Telecom International a perdu plus de 4 millions de dollars de revenus et a dépensé 2,6 millions de dollars afin de réparer la liaison sous-marine manquante. Cet incident s'inscrit dans une série de vols de câbles commis au Vietnam en 2007 par cinq groupes différents de pirates spécialisés dans ce type de vol. Si cet incident a été attribué à des pêcheurs locaux, il n'est pas confirmé que les bris de câbles soient intentionnels ou accidentels.[129] D'autres sources soutiennent que, au total, des pêcheurs vietnamiens auraient volé plus de 500 kilomètres de câbles sous-marins en 2007.[130] Le Vietnam est en effet confronté à de nombreuses ruptures accidentelles de câbles. Les quelques exemples suivants illustrent la fréquence de ces incidents et leurs impacts. Le 27 août 2017, trois câbles sous-marins du Vietnam ont été rompus de manière simultanée, perturbant grandement le trafic Internet du pays avec l'étranger.[131] En 2017, le Vietnam avait quatre câbles le connectant à l'international, contre un total de cinq aujourd'hui. Les câbles en question sont le SMW3, l'AAG et l'Intra Asia. L'AAG relie l'Asie du Sud-Est aux États-Unis et représentait, en 2017, 60 % du débit Internet international du Vietnam. L'Intra Asia relie le Vietnam à Singapour, aux Philippines, à Hong Kong et au Japon. Le SMW3 relie, quant à lui, le Vietnam aux pays d'Asie de l'Est, du

[127] *Ibid.*, p. 14-24.
[128] *Ibid.*, p. 25.
[129] *Ibid.*, p. 14.
[130] Photonics. (2007, 8 juin). Cable Theft Costs Vietnam $6M. *Photonics* (Ho Chi Minh, Vietnam). <https://www.photonics.com/Articles/Cable_Theft_Costs_Vietnam_6M/a29904>.; Morel, C. (2023), *Op. cit.*, p. 83-84.
[131] Linh, T. (2017, 29 août). Internet : trois câbles sous-marins du Vietnam endommagés. *Le Courrier du Vietnam*. <https://lecourrier.vn/internet-trois-cables-sous-marins-du-vietnam-endommages/424355.html>.; Morel, C. (2023), *Op. cit.*, p. 83.

Moyen-Orient et de l'Europe de l'Ouest.[132] En février 2023, les cinq câbles du Vietnam ont été endommagés, entraînant une perte de 75 % du transit numérique du pays.[133] Le 15 juin 2024, trois des cinq câbles du Vietnam ont arrêté de fonctionner, posant un sérieux problème en termes de connexion Internet. Les trois câbles affectés sont la connexion Intra Asia vers Singapour, la liaison Asia Pacific Gateway (APG) et la liaison AAE-1. Ces interruptions sont attribuées à des causes non intentionnelles, comme la dégradation naturelle des câbles au fil du temps ou les dommages causés accidentellement par des navires.[134] Que les causes soient naturelles ou non, les incidents auxquels font face les câbles sous-marins deviennent de plus en plus fréquents.[135]

En juin 2010, un incident jugé probablement intentionnel est survenu aux Philippines, perturbant ainsi l'accès à Internet dans le pays. Un groupe de séparatistes et de terroristes serait à l'origine des coupures sur le câble reliant les Philippines au Japon. L'acte a eu lieu près de Cagayan de Oro, sur la terre ferme et près des côtes. La cause ou l'origine des coupures n'a pas officiellement été attribuée.[136] En mars 2013, le bris intentionnel d'un câble en Indonésie a été officiellement attribué à des criminels. Au total, 16 tonnes et 31,7 kilomètres de câbles sous-marins ont été volés entre l'île de Bangka et l'île de Riau en Indonésie. Les services de communication vocale et de données ont été perturbés pendant plus d'un mois.[137] Ces deux cas concernent des groupes terroristes ou criminels, donc des acteurs non étatiques. C'est pourquoi ils ne sont pas davantage détaillés.

En février 2023, deux câbles sous-marins approvisionnant Taïwan ont été endommagés. Le 2 février, le câble Taima #2 près de Dongyin dans les îles Matsu a été endommagé par un navire de pêche chinois. Le 8 février, c'est le câble Taima #3, situé près de Juguang, qui a été endommagé par un cargo chinois. Les coupures se sont produites à 10 milles nautiques du littoral chinois, ce qui correspond à une distance de moins de 19 kilomètres. Ces incidents ont entraîné six semaines de panne d'Internet et d'isolement numérique sur l'île de Matsu. Les 14 000 citoyens avaient un accès très limité à Internet et une connexion lente. Les activités des entreprises locales ont

[132] Linh, T., *Op. cit.*
[133] Noor, E., Subsea Communication Cables in Southeast Asia*, Op. cit.*, p. 4.
[134] Connatser, M. (2024, 18 juin). Vietnam's internet again in trouble as three of five submarine cables go down. *The Register*. <https://www.theregister.com/2024/06/18/vietnam_internet_cables/>.
[135] Linh, T., *Op. cit.*
[136] Beyer, J. L. *et al*., *Op. cit.*, p. 17.
[137] *Ibid.*

également été ralenties par la panne. La réparation du câble a coûté entre 660 000 et 1,3 million de dollars à l'entreprise taïwanaise Chunghwa Telecom. Si l'incident est présumé être intentionnel, le manque de preuves ne permet pas de qualifier cette situation comme étant une attaque. L'origine des coupures est toutefois attribuée à des navires chinois, c'est-à-dire qu'ils sont immatriculés et enregistrés comme étant chinois.[138] Ce genre d'incidents répétés nuit à la réputation de Taïwan comme chef de file dans le domaine des technologies numériques. En effet, la répétition des ruptures de câbles normalise les perturbations d'activités quotidiennes qui nécessitent une connexion Internet stable. À la suite des incidents de 2023, Taïwan a qualifié les câbles sous-marins comme des infrastructures critiques et a installé un système d'alerte automatique entre l'île principale taïwanaise et les îles Matsu. En outre, Taïwan a durci sa loi sur la gestion des télécommunications afin d'appliquer des sanctions plus sévères en cas de dommages causés aux câbles.[139] Pékin a affirmé que l'incident de 2023 était une coïncidence, accusant Taipei de manipuler les faits. Le détroit de Taïwan est l'un des plus empruntés au monde, avec plus de 1 000 cargos transitant par cette voie chaque semaine. Les accidents sont donc probables, mais les perturbations de 2023 et des navires immatriculés en Chine naviguant à proximité de câbles importants sèment le doute. Ce doute caractérise les opérations en zone grise.[140]

Plus récemment, Taïwan a été confronté à plusieurs incidents. Le 3 janvier 2025, le câble Trans Pacific Express (TPE) a été endommagé au large des côtes de Keelung par le navire Shunxing 39. Seulement quatre fibres optiques ont été touchées, alors la connectivité a été maintenue et les données ont été rapidement redirigées vers d'autres câbles. Encore une fois, le manque de preuves ne permet pas de qualifier cette situation d'attaque intentionnelle, même si elle est présumée l'être. Dans ce cas-ci, l'origine de l'incident a été partiellement attribuée : si le cargo appartient à Hong Kong, il est immatriculé en Tanzanie et/ou au Cameroun et est doté d'un équipage chinois. Le navire est donc tout de même soupçonné d'appartenir à la Chine.[141] La garde côtière taïwanaise a été avertie de l'incident par la compagnie Chunghwa Telecom, qui avait remarqué un bateau

[138] Beyer, J. L. *et al*., *Op. cit.*, p. 19. ; Quốc Tế, B. (2024, 29 décembre). Câble optique - Système d'armes sous-marines stratégiques. *Vietnam.vn*. <https://www.vietnam.vn/fr/cap-quang-he-vu-khi-chien-luoc-duoi-long-bien>.
[139] Kim, J., Kim, H. et Terasawa, M. (2025, 16 mai). The World's Subsea Cables Are Under Threat. Can Canada Help Protect Them? *Asia Pacific Foundation of Canada*. <https://www.asiapacific.ca/fr/publication/les-cables-sous-marins-du-monde-entier-sont-menaces-le>.
[140] Ocon, J. et Walberg, J. (2025). China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities. *Global Taiwan Institute, 10*(11), 9-12. <https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/>, p. 10.
[141] Beyer, J. L. *et al*., *Op. cit.*, p. 22.

naviguant sur les mêmes routes que les câbles sous-marins. La garde côtière taïwanaise a ensuite intercepté le navire, qui possédait d'ailleurs deux systèmes d'identification automatique (AIS – Automatic Identification System), ajoutant un élément au comportement suspect du navire.[142] Cet exemple révèle une tendance plus large. De nombreux navires chinois s'engagent dans des activités illicites, notamment en désactivant leur AIS, ou encore en utilisant des pavillons de complaisance (aussi appelés pavillons de « libre immatriculation ») afin de camoufler leur nationalité d'origine. Ces actions les rendent plus difficiles à repérer et à identifier. À la suite de cet incident, Taïwan cherche à instaurer des inspections plus strictes concernant les navires étrangers.[143] Par ailleurs, Taïwan a pu collaborer de manière bilatérale avec des alliés de la région, soit la Corée du Sud et le Japon. En janvier, Taipei a fait appel à l'appui de Séoul afin d'enquêter sur un navire chinois qui aurait potentiellement coupé des câbles et qui se rendait ensuite à Busan, une ville portuaire en Corée du Sud. Le Japon a non seulement publié une déclaration condamnant la rupture de câbles survenue le 3 janvier, mais a également envoyé un navire de type destroyer dans le détroit de Taïwan le 5 janvier. Ce geste est particulièrement symbolique, car il s'agit de la première fois qu'un navire de la Force maritime d'autodéfense japonaise traverse le détroit de Taïwan, en solidarité avec l'île taïwanaise et pour affirmer son engagement à assurer la stabilité dans le détroit.[144]

Le 25 février 2025, un peu après 3h00 du matin, Chunghwa Telecom a détecté la rupture d'un câble reliant l'île principale de Taïwan aux îles Penghu. Chunghwa Telecoms a contacté la garde côtière taïwanaise qui, vers 2h30 du matin, suivait déjà le cargo Hong Tai. Celui-ci était initialement enregistré sous le nom de Hong Tai 58, alors que la coque du navire indiquait Hong Tai 168. Le navire est immatriculé au Togo, mais est soupçonné d'avoir une appartenance chinoise et tous les membres de l'équipage sont identifiés comme étant des ressortissants chinois. Le Hong Tai a été guidé vers le port d'Anping, à Tainan, où son équipage a été arrêté et le navire saisi par la garde côtière taïwanaise. La connexion numérique et la communication n'ont pas été interrompues entre Taïwan et les îles Penghu, Chunghwa Telecom ayant redirigé les données vers d'autres câbles. Si la situation est soupçonnée d'être une attaque intentionnelle, l'origine de l'incident est

[142] Baum, A., Salgame, N. et Zolyniak, A. (2025, 11 février). Water Wars: Trump, Taiwan, and the Philippines. *The Lawfare Institute*. <https://www.lawfaremedia.org/article/water-wars--trump--taiwan--and-the-philippines>.
[143] Kim, J., Kim, H. et Terasawa, M., *Op. cit.*
[144] *Ibid.*

partiellement attribuée à la Chine.[145] En septembre 2025, Taïwan a approuvé l'amendement de sept lois afin de renforcer la protection des infrastructures critiques, incluant les câbles sous-marins de télécommunications, contre les actes de sabotage étrangers. Ces amendements visent à augmenter les pénalités encourues pour les dommages intentionnels causés à ces infrastructures, à assurer la sécurité nationale, à maintenir les services essentiels et à dissuader la désactivation de l'AIS.[146] Les amendements de 2023 à la loi taïwanaise sur la gestion des télécommunications ont permis de condamner le capitaine du navire Hong Tai 58 à trois ans de prison pour avoir volontairement sectionné un câble sous-marin, créant ainsi un précédent juridique.[147] Face à la multiplication des incidents visant ses infrastructures sous-marines, Taïwan renforce sa stratégie de défense des câbles. En effet, le nouveau budget de la garde côtière taïwanaise, d'un montant total de 972 millions de dollars américains, prévoit des fonds destinés à la protection des câbles sous-marins. Plusieurs projets câblés sont en cours, notamment à l'est de l'île, ce qui permettra à Taïwan de diminuer sa vulnérabilité face aux attaques chinoises dans le cadre d'un conflit potentiel. Parmi les projets, certains sont soutenus par Google et Meta et visent à connecter Taïwan aux Philippines, au Japon, ainsi qu'à la côte ouest des États-Unis.[148] Cela témoigne de l'influence majeure des États-Unis et des entreprises américaines sur le réseau mondial de câbles, tout en exprimant la manière dont les États-Unis peuvent utiliser ces câbles comme outils d'influence. De plus, il est important de noter que, depuis 2017, environ 30 ruptures de câbles causées par la Chine ont été recensées à Taïwan. Ces incidents ne sont pas inclus dans la présente étude, car ils sont considérés comme accidentels. Cependant, la multiplication des dommages causés aux câbles taïwanais entretient le flou et sème le doute quant aux réelles intentions de la Chine.[149] Une fois de plus, cela illustre les méthodes en zone grise de Pékin. D'ailleurs, Taïwan se montre de plus en plus vigilant face aux tactiques en zone grise de la Chine, notamment en assurant des patrouilles côtières 24 heures sur

[145] Beyer, J. L. *et al*., *Op. cit.*, p. 24.
[146] Tzu-ti, H. (2025, 19 septembre). Taiwan proposes tougher laws to protect undersea cables. *Taiwan News* (Taipei). <https://taiwannews.com.tw/en/news/6203736>.
[147] Indo-Pacific Defense FORUM. (2025, 28 septembre). Taiwan strengthens patrols against China's undersea cable sabotage. *Indo-Pacific Defense FORUM*. <https://ipdefenseforum.com/2025/09/taiwan-strengthens-patrols-against-chinas-undersea-cable-sabotage/>.
[148] Rinaldi, T. (2025, 10 septembre). Taiwan advances undersea cable defense strategy. *Taiwan News* (Taipei). <https://taiwannews.com.tw/en/news/6197737>.
[149] Beyer, J. L. *et al*., *Op. cit.*, p. 29.

24 et une surveillance accrue des bateaux chinois ou liés à la Chine qui figurent sur une liste noire.[150]

La difficulté d'attribuer la cause ou l'origine d'une attaque intentionnelle contre les câbles sous-marins s'explique, entre autres, par des facteurs juridiques. Il existe en effet un manque de mécanismes d'application de la loi, particulièrement dans les eaux internationales ou dans les zones revendiquées par plusieurs acteurs étatiques. La Convention de 1884 pour la protection des câbles télégraphiques sous-marins, ainsi que l'article 21 de la Convention des Nations unies sur le droit de la mer, n'offrent pas de règlement précis et ne proposent que des protections partielles.[151] D'ailleurs, les câbles sous-marins militaires sont soumis aux mêmes instruments juridiques internationaux que les câbles civils, ce qui s'inscrit dans un débat plus large quant au droit ou non de recourir à des activités militaires (incluant l'usage de câbles militaires) dans la ZEE et sur le plateau continental.[152] De plus, plusieurs États n'ont pas de législation en place pour rendre criminels les dommages intentionnels perpétrés contre les câbles.[153] À l'échelle internationale, le risque que posent les groupes terroristes envers les câbles sous-marins de télécommunications n'a pas encore été reconnu, ce qui se traduit par un manque de régime juridique pour ce genre d'enjeux.[154]

En résumé, les cas taïwanais peuvent être qualifiés d'actions directes causées par un acteur étatique ayant agi par l'intermédiaire d'individus distincts de l'État. Les actions directes visent l'infrastructure physique de câbles et l'auteur étatique de ces actes serait la Chine agissant par l'intermédiaire d'un tiers.[155] Taïwan a réagi de diverses manières face aux actes de sabotage chinois visant ses câbles sous-marins. En 2023, la qualification de ces câbles en tant qu'infrastructures critiques ainsi que le renforcement de la législation taïwanaise sur la gestion des télécommunications constituent des mesures supplémentaires visant à assurer une meilleure protection juridique de ces liaisons sous-marines. L'installation d'un système d'alerte automatique

[150] Indo-Pacific Defense FORUM, *Op. cit.*
[151] Kim, J., Kim, H. et Terasawa, M., *Op. cit.*
[152] Roach, J. A., *Op. cit.*, p. 343-344.
[153] Beckman, R. (2014). Chapter 12. Protecting Submarine Cables from Intentional Damage – The Security Gap. Dans D. R. Burnett, R. Beckman et T. M. Davenport (dir.), *Submarine Cables - The Handbook of Law and Policy* (p. 281-297). Brill. <https://doi.org/10.1163/9789004260337_014>, p. 281.
[154] *Ibid.*, p. 297.
[155] Morel, C. (2019), *Op. cit.*, p. 38.

entre l'île principale de Taïwan et les îles Matsu permet d'assurer une réaction rapide en cas d'incidents similaires à l'avenir. En janvier 2025, Taïwan vise à renforcer les inspections des navires étrangers et collabore de manière bilatérale avec des alliés tels que la Corée du Sud et le Japon. Suivant l'incident de février 2025, Taïwan amende sept lois afin de renforcer la protection des câbles sous-marins contre le sabotage étranger. En plus de l'aspect juridique, Taipei cherche également à lutter davantage contre les navires fantômes qui désactivent leur AIS et à renforcer sa stratégie de défense, notamment en allouant des parts du budget de la garde côtière taïwanaise à la protection des câbles sous-marins. Les réactions de Taïwan témoignent d'un intérêt stratégique croissant pour les infrastructures critiques sous-marines de télécommunications. En effet, l'archipel cherche à dissuader et à prévenir les actes de sabotage, tout en améliorant sa réponse face à de tels incidents afin d'être plus rapide et efficace, et ainsi éviter toute perturbation des services essentiels, particulièrement dans le cas d'éventuelles attaques chinoises.[156] Les mesures de sécurisation adoptées par Taïwan en réponse à ces incidents constituent un exemple de la manière dont ces infrastructures critiques sont protégées contre les menaces extérieures. Les actions entreprises par la Chine et les États-Unis montrent que ces câbles sont également utilisés comme outils au service des intérêts nationaux et comme vecteurs d'influence et de menace.

Concernant les trois derniers incidents survenus à Taïwan, plusieurs auteurs sont d'avis que ces événements s'inscrivent dans la stratégie en zone grise de la Chine, dont l'objectif est de nuire petit à petit à la stabilité de Taïwan. En faisant usage de moyens non militaires, la Chine exerce une certaine pression sur Taïwan tout en évitant un conflit direct.[157] Le caractère confus et flou des opérations en zone grise permet de fournir un autre élément d'explication concernant la difficulté d'attribuer. En outre, l'attribution est souvent compliquée en raison de la difficulté à recueillir suffisamment de preuves pour confirmer l'intention de nuire.[158] Ainsi, les actes de sabotage présumés sont souvent non attribués ou bien qualifiés comme étant des accidents résultant de l'activité maritime et humaine.[159] Depuis 2022, les experts observent une tendance croissante à attribuer rapidement les incidents à des États, c'est-à-dire que l'attribution est souvent basée sur les tensions géopolitiques avant d'avoir pleinement effectué des enquêtes approfondies sur les

[156] Indo-Pacific Defense FORUM, *Op. cit.*
[157] Ocon, J. et Walberg, J., *Op. cit.*, p. 11.
[158] Beyer, J. L. *et al*., *Op. cit.*, p. 25.
[159] *Ibid.*, p. 26.

incidents.[160] Bueger et Liebetrau corroborent ces propos en appelant à la prudence. Les discours sur les menaces semblent reposer sur des évaluations générales du contexte géopolitique, plutôt que sur des incidents confirmés survenus précédemment. Les perceptions des menaces comportent le risque d'être exagérées et de surévaluer les risques, favorisant ainsi de potentielles réponses disproportionnées. C'est pourquoi il est également essentiel de se pencher sur les vulnérabilités réelles du réseau de câbles, et pas uniquement sur les risques potentiels.[161] Le sabotage initié par un État constitue tout de même une menace émergente. Les États ayant des capacités avancées en eaux profondes ou en haute mer, tels que la Russie et la Chine, ont l'habilité de nuire au fonctionnement des câbles sous-marins. Comme susmentionné, ces actes de sabotage peuvent facilement être confondus avec des incidents maritimes de routine, ce qui complique l'identification d'une attaque et son attribution.[162] En résumé, le sabotage des câbles sous-marins, qu'il soit physique ou via une cyberattaque, peut être très difficile à identifier comme tel et à attribuer.[163] La prochaine sous-section traite de la concurrence numérique sino-américaine dans la région, ainsi que dans le cas des câbles sous-marins de Taïwan.

3.3 L'Asie du Sud-Est et la mer de Chine méridionale, théâtres de la concurrence sino-américaine

Cette sous-section traite de la région du sud-est asiatique et de la MCM comme des théâtres de la concurrence sino-américaine. L'importance stratégique de Taïwan est d'abord décrite, puis le rôle des entreprises du secteur câblé, notamment américaines et chinoises, est abordé. Ensuite, les stratégies américaines et chinoises sont étudiées et mises en relation avec le cas de Taïwan, ce qui montre comment les câbles peuvent également être des instruments d'influence et de menace.

L'Asie du Sud-Est est bien connue pour être au cœur de la rivalité sino-américaine et un théâtre de tensions entre les deux premières puissances économiques mondiales. Taïwan se retrouve d'ailleurs au cœur de la concurrence numérique entre la Chine et les États-Unis. Alors que Taïwan souhaite s'affirmer sur la scène internationale comme un État souverain, la Chine considère l'archipel comme une province ayant un statut particulier et qui doit être réunifiée ou annexée à la

[160] *Ibid.*, p. 25.
[161] Bueger, C. et Liebetrau, T., *Op. cit.*, p. 396.
[162] Beyer, J. L. *et al*., *Op. cit.*, p. 37.
[163] Botting, A. et Jordan-Zoob, I. (2024, 28 février). Optical Core Infrastructure: The Hidden Highway of Connectivity. *Wilson Center*. <https://www.wilsoncenter.org/article/optical-core-infrastructure-hidden-highway-connectivity>.

Chine continentale. Pékin ne reconnaît donc pas l'indépendance de Taipei, mais est tout à fait consciente de son intérêt stratégique. Taïwan représente un enjeu stratégique majeur, car elle détient un quasi-monopole sur la production de microprocesseurs, des éléments essentiels de toutes technologies, qu'il s'agisse de téléphones portables, de centres de données, d'équipements médicaux, de satellites ou encore de systèmes militaires. La Taiwan Semiconductor Manufacturing Company (TSMC) assure près de 90 % de la production mondiale de puces électroniques. Ainsi, le contrôle de Taïwan permet d'assurer à la Chine une domination technologique mondiale. Ceci est un élément explicatif du durcissement de la position de Pékin vis-à-vis de Taïwan, qui se manifeste au travers de campagnes de désinformation, de violations de l'espace aérien et maritime taïwanais, ou de ruptures de câbles sous-marins. Les États-Unis sont également conscients de l'intérêt stratégique que représente Taïwan. En 2023, le gouvernement américain a dédié une enveloppe de 2 milliards de dollars à Taïwan, dans l'objectif d'éviter un déséquilibre technologique et militaire entre Taipei et Pékin. Vu l'importance de Taïwan dans la production de puces électroniques, un tel déséquilibre nuirait à la sécurité nationale des États-Unis.[164]

De plus, il existe des inégalités quant à la répartition physique des câbles à l'échelle internationale, ce qui crée des enjeux politiques et des dépendances.[165] Certains acteurs sont donc avantagés par rapport à d'autres quant à une certaine domination de l'information, l'accès matériel à la fibre optique garantissant un accès immatériel à l'information.[166] Des zones à forte densité de câbles, comme les détroits de Malacca, de Luçon ou de Suez, contrastent brutalement avec des zones caractérisées par des déserts câblés.[167] En 2021, autour de 98 % du réseau international de câbles sous-marins était produit et posé par quatre entreprises privées, soit la compagnie américaine SubCom, l'entreprise française Alcatel Submarine Networks (ASN), la société japonaise Nippon Electric Company (NEC) et la firme chinoise HMN Tech.[168] Les géants d'Internet sont Google, Apple, Facebook, Amazon et Microsoft, également surnommés « GAFAM ». Ceux-ci représentent

[164] Bastien-Carignan, N., Girard, P. et Lecchino, M. (2025, 14 juillet). Débranchez Taïwan, et le monde s'éteint. *Le Devoir*. <https://www.ledevoir.com/opinion/idees/900046/idees-debranchez-taiwan-monde-eteint>. ; Eurasia Group. (2020). *The Geopolitics of Semiconductors*. <https://www.eurasiagroup.net/live-post/geopolitics-semiconductors>.
[165] Morel, C. (2019), *Op. cit.*, p. 42.
[166] Morel, C. (2017). Les câbles sous-marins : un bien commun mondial ? *Études*, (3), 19-28. <https://doi.org/10.3917/etu.4236.0019>, p. 21.
[167] *Ibid.*, p. 25.
[168] Quốc Tế, B., *Op. cit.* ; Kim, J., Kim, H. et Terasawa, M., *Op. cit.*

la majorité du trafic de données qui passe par câble sous-marin.[169] Environ la moitié de la bande passante de ce réseau de câbles sous-marins est actuellement la propriété de Google, Meta (qui est lié à Facebook), Amazon ou Microsoft, ou est louée par ces entreprises.[170] La compagnie privée Huawei Technologies s'est séparée de son ancienne filiale Huawei Marine Networks, qui est maintenant une entreprise nationale chinoise nommée HMN Tech.[171] En outre, l'armée chinoise a acquis un navire dédié au secteur câblé en 2015, ce qui exprime l'accroissement de l'usage militaire de ces infrastructures par la Chine. Concernant les États-Unis, un tournant est également observable vers 2015, les entreprises GAFAM ayant commencé à investir davantage dans les câbles sous-marins.[172] Ainsi, le réseau mondial de communication et d'information, dont la forme physique se matérialise notamment par les câbles sous-marins, est un lieu qui exprime des rapports de force et des relations de pouvoir. Morel rappelle que, lorsque la Grande-Bretagne dominait le secteur des communications télégraphiques au XX^{e} siècle, les autres puissances étatiques, telles que la France, l'Allemagne et les États-Unis, ont mis en œuvre diverses stratégies d'évitement. Ces stratégies visaient à contourner les interceptions de communications internationales orchestrées par la Grande-Bretagne.[173] Aujourd'hui, de nombreuses entreprises privées adoptent une stratégie similaire en évitant la MCM en raison des tensions géopolitiques et des revendications territoriales divergentes dans la région.[174]

Les inégalités du réseau révèlent les rapports de force et les dynamiques de pouvoir, ainsi que la rivalité sino-américaine en matière de supériorité technologique en Asie du Sud-Est et en MCM. Les stratégies américaines sont d'abord abordées, suivies par celles de la Chine. Ces stratégies permettent de mieux comprendre la concurrence numérique sino-américaine et sa relation avec Taïwan.

[169] Morel, C. (2021). Sous la mer, le monde numérique : Une géopolitique des câbles sous-marins. *Questions internationales, 1*(107-108), 81-87. <https://doi.org/10.3917/quin.107.0081>.
[170] Quốc Tế, B., *Op. cit.*
[171] Brock, J., *Op. cit.*
[172] McGeachy, H., *Op. cit.*, p. 166.
[173] Morel, C. (2019), *Op. cit.*, p. 41.
[174] Starosielski, N., *Op. cit.*, p. 29.

3.3.1 Les stratégies des États-Unis

La stratégie des États-Unis consiste à renforcer les liens entre les sphères publique et privée dans le domaine câblé, de sorte à faciliter une réponse coordonnée en cas de dommages ou d'attaques contre le réseau. Étant situés au centre de la toile de câbles sous-marins, les États-Unis ont tout intérêt à protéger leur réseau et à assurer une gestion efficace des dommages.[175] De plus, la notion de « découplage » (ou *decoupling* en anglais) est une stratégie principalement menée par les États-Unis qui consiste à séparer intentionnellement les chaînes d'approvisionnement et les centres de fabrication américains et chinois.[176]

Les États-Unis occupent une place privilégiée au sein du réseau mondial, l'information circulant de manière prioritaire sur leur territoire. Ceci n'est évidemment pas un choix conscient, puisque les capacités du réseau font en sorte que les données trouvent un avantage numérique à transiter par les États-Unis. Malgré cela, il est normal que des questionnements émergent concernant la neutralité et la maîtrise de l'information. Plusieurs auteurs considèrent la politique américaine de développement d'infrastructures câblées comme un moyen agressif d'asseoir leur domination mondiale sur l'information et de propager leur diplomatie culturelle.[177] Les États-Unis sont le pays ayant le plus de câbles sous-marins, avec un total de 48 liaisons sur leur territoire national en 2020. Ainsi, les États-Unis occupent effectivement une place centrale au sein du réseau mondial de câbles et au sein de « l'économie d'Internet et de l'information ». De nombreux États dépendent des États-Unis pour leur Internet, comme c'est le cas des pays d'Amérique du Sud pour leurs communications avec l'Asie et l'Europe. En effet, l'Amérique du Sud ne possède pas de câbles la reliant directement aux continents asiatiques et européens, ce qui entraîne un passage quasi-obligatoire des données internationales via les États-Unis. Washington est un acteur très compétitif dans le domaine, ayant fait en sorte que l'information transite principalement par l'Amérique du Nord. La National Security Agency (NSA), soit l'agence américaine de renseignement intérieur, a une juridiction qui favorise son contrôle sur l'information et la captation des communications transitant sur le territoire américain. De plus, le Groupe des cinq (*Five Eyes*) permet à Washington d'élargir son champ d'influence et son accès aux communications ne transitant pas sur son

[175] Morel, C. (2019), *Op. cit.*, p. 42.
[176] McGeachy, H., *Op. cit.*, p. 165.
[177] Morel, C. (2017), *Op. cit.*, p. 23-24.

territoire.[178] L'alliance *Five Eyes* est un partenariat qui permet le partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.[179] Ainsi, les États-Unis ont tout intérêt à maintenir le statu quo et leur position de force ou de supériorité dans le domaine des câbles sous-marins, notamment en raison de leur accès privilégié à l'information et aux communications. À l'inverse, des initiatives visant à s'émanciper de cette dépendance vis-à-vis des États-Unis émergent petit à petit, de nombreux États souhaitant assurer leur souveraineté numérique en diversifiant leurs liaisons sous-marines de communication vers l'international. Malgré des tentatives de rééquilibrer la cartographie mondiale des câbles sous-marins, les États-Unis restent premiers dans le domaine. Ceci illustre une autre inégalité du réseau mondial, c'est-à-dire que la plupart des acteurs bien connectés en termes de câbles, et donc de TIC et d'Internet, sont occidentaux.[180] Le réseau mondial de câbles reflète l'état de la scène internationale : en l'absence de gouvernance mondiale, les acteurs les plus forts se sont imposés afin d'en dicter les règles.[181] Les câbles peuvent donc également servir d'outils d'influence.

L'expansion de l'influence chinoise dans le domaine des infrastructures de télécommunications, dont les câbles sous-marins, comporte un certain risque pour les États-Unis. Comme susmentionné, de grandes quantités de données transitent par les câbles de fibre optique, que ce soit de nature gouvernementale, financière ou privée. Le contrôle de ces câbles par des entreprises chinoises signifie que le gouvernement chinois a un accès facilité à de telles données. Ainsi, le contrôle croissant de la Chine sur les données représente un risque stratégique pour les États-Unis et leurs alliés, tout en impliquant des craintes d'espionnage.[182] Une enquête menée par Reuters montre une tendance croissante de la part des États-Unis à intervenir afin d'empêcher les firmes chinoises de signer des contrats privés qui relieraient le réseau américain à celui de la Chine en Asie-Pacifique. Ceci s'inscrit dans la stratégie américaine de découplage mentionnée précédemment. S'ils n'empêchent pas la signature des contrats, les États-Unis demandent le changement d'itinéraire ou l'abandon de certains câbles pour le même objectif, soit éviter la connexion avec le réseau chinois.

---

[178] Morel, C. (2021), *Op. cit.*
[179] Leymarie, P. (2022, 1er mars). Le club des « cinq » face à la Chine. *Le Monde diplomatique*, p. 11. <https://www.monde-diplomatique.fr/2022/03/LEYMARIE/64415>.
[180] Morel, C. (2017), *Op. cit.*, p. 25.
[181] *Ibid.*, p. 26.
[182] Harding, B. (2019, 15 février). China's Digital Silk Road and Southeast Asia. *Center for Strategic and International Studies (CSIS)*. <https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia>.

La Chine a progressivement amenuisé l'autonomie de Hong Kong, ce qui explique les craintes vis-à-vis de ce territoire.[183] Face à la montée en notoriété de la Chine dans ce domaine, les entreprises américaines répliquent en augmentant leurs investissements. Par exemple, en février 2023, l'entreprise américaine SubCom a investi 600 millions de dollars destinés à la construction d'un câble sous-marin de 19 000 kilomètres reliant la France et Singapour. La firme chinoise Heiman avait obtenu l'appel d'offres pour ce projet, ainsi que le soutien en capitaux de China Telecom, China Mobile et China Unicom. Par contre, sous la pression de Washington, l'investisseur du projet avait dû transférer le contrat à US SubCom.[184] De plus, depuis 2020, les États-Unis ont annulé plusieurs projets et détourné des trajectoires de câbles, de crainte que la Chine ne puisse récolter des renseignements et des données américaines. C'est notamment le cas pour des câbles reliant les États-Unis à Hong Kong.[185] Le refus de construire un nouveau câble entre le territoire américain et Hong Kong exprime un renforcement de la position de Washington vis-à-vis de la protection de ses intérêts de sécurité nationale contre les capacités croissantes de la Chine en matière d'infrastructure d'Internet.[186] Ainsi, les entreprises américaines que sont les GAFAM alignent leurs actions aux intérêts du gouvernement américain. Par exemple, en 2021, Google et Meta ont accepté de conclure un accord de sécurité nationale avec le gouvernement américain. Ils se sont engagés à exclure les partenaires associés à la Chine de leurs projets et à diversifier les interconnections en Asie, notamment avec la Thaïlande, le Vietnam, Singapour, l'Indonésie et les Philippines.[187] Ces exemples montrent que les fonds marins deviennent de plus en plus le théâtre de la compétition entre les grandes puissances, et plus particulièrement entre les États-Unis et la Chine. Le cas de Taïwan ne fait pas exception. En effet, des entreprises américaines travaillent actuellement sur des projets de construction de câbles à l'est de l'île, ce qui vise notamment à renforcer la défense des câbles taïwanais.[188] Les stratégies des États-Unis illustrent la manière dont ils étendent leur influence à travers les câbles. La prochaine sous-section se concentre sur la stratégie chinoise.

---

[183] Brock, J. (2023, 24 mars). U.S. and China wage war beneath the waves - over internet cables. *Reuters* (Singapore). <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>.
[184] Quốc Tế, B., *Op. cit.*
[185] Quốc Tế, B., *Op. cit.*; McGeachy, H., *Op. cit.*, p. 170.
[186] McGeachy, H., *Op. cit.*, p. 174.
[187] Kang, J. et Jacob, J. (2024). *Connecting the Indo-Pacific: The future of subsea cables and opportunities for Australia*. Australian Strategic Policy Institute (ASPI). <https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/>, p. 8.
[188] Rinaldi, T., *Op. cit.*

3.3.2 La stratégie de la Chine et la route de la soie numérique

En 2013, la Chine a lancé la « Belt and Road Initiative » (BRI – Nouvelle route de la soie), un vaste projet d'infrastructures d'envergure mondiale visant à accroître l'influence internationale de la Chine. Lancée en 2015, l'initiative chinoise « Digital Silk Road » (DSR – Route de la soie numérique) permet de préciser le volet numérique de la BRI, tout en fournissant un soutien de la part de l'État chinois à certaines entreprises nationales du domaine technologique. L'objectif est d'accroître la capacité de la Chine à participer aux instances internationales chargées de définir les normes technologiques et les règles de gouvernance.[189] La stratégie numérique de la Chine est mise en œuvre à travers ses entreprises nationales, telles que Huawei, ZTE, Alibaba et Tencent. Les entreprises chinoises HMN Tech et ZTE sont les principales impliquées au niveau des infrastructures soutenant les TIC, notamment les câbles de fibre optique. En 2019, HMN Tech avait complété plus d'une douzaine de projets de câbles sous-marins en Asie du Sud-Est et travaillait sur près d'une vingtaine d'autres projets du genre, principalement aux Philippines et en Indonésie.[190] L'initiative DSR vise à faire de la Chine un acteur de premier plan en termes numériques, notamment en remportant 60 % du marché mondial de câbles sous-marins. En ciblant les pays émergents d'Asie, du Pacifique, du Moyen-Orient et d'Afrique, l'entreprise chinoise HMN Tech a pu croître rapidement. En effet, l'entreprise fournissait 11 % de la longueur totale des câbles sous-marins en 2021, contre 18 % en 2024. La stratégie de la Chine a donc fonctionné, faisant du pays le premier fournisseur et propriétaire mondial de câbles sous-marins.[191]

Les revendications territoriales divergentes en MCM restreignent les compagnies technologiques du secteur câblé. Le UNCLOS garantit la souveraineté des États sur les câbles sous-marins se trouvant dans leur ZEE. Ainsi, si une entreprise souhaite développer son réseau de câbles dans la région, elle doit préalablement obtenir l'autorisation de tous les États ayant des revendications territoriales sur la zone en question. Les États ont des interprétations différentes de ce qui constitue leurs frontières légales, alors les entreprises privées doivent également se conformer aux lois dans chacun des pays. En MCM, le Brunei, l'Indonésie, les Philippines, le Vietnam, la Chine et Taïwan

[189] Greene, R. et Triolo, P. (2020, 8 mai). Will China Control the Global Internet Via its Digital Silk Road? *Carnegie Endowment for International Peace & SupChina*. <https://carnegieendowment.org/posts/2020/05/will-china-control-the-global-internet-via-its-digital-silk-road?lang=en>.
[190] Harding, B., *Op. cit.*
[191] Quốc Tế, B., *Op. cit.*

ont tous des revendications territoriales et maritimes divergentes, ce qui complique la tâche pour les compagnies du secteur câblé. De nombreuses compagnies prennent donc la décision d'éviter la MCM afin de pallier l'incertitude géopolitique et les négociations ardues avec chacun des États pour l'obtention des permis. En conséquence, les coûts et les délais augmentent en raison des détours. D'ailleurs, les navires chargés de la réparation des câbles doivent également obtenir des permis de la part de tous les États concernés afin d'opérer dans les zones contestées, ce qui ajoute une autre difficulté pour le réseau de câbles dans la région.[192] Or, en évitant la MCM, les entreprises privées font progresser la campagne chinoise d'affirmation de souveraineté sur les eaux contestées, et donnent l'opportunité à Pékin d'influencer la gestion des câbles tout en assurant la participation de ses entreprises nationales.[193] En effet, alors que la Chine dissuade les entreprises étrangères de poser des câbles dans ses territoires revendiqués, ceci lui permet de développer son propre secteur public de construction de câbles dans la MCM. L'entreprise nationale HMC Tech est un exemple de la capacité de la Chine à influencer la configuration du réseau de câbles sous-marins. De cette manière, la Chine peut concentrer le passage massif de données dans des territoires sous sa juridiction. Un monopole chinois sur les câbles sous-marins en MCM accroît le risque que la Chine utilise ces infrastructures comme outils au service d'une politique étrangère hostile et agressive. Desurmont explique que la Chine pourrait inciter les États de la MCM à abandonner leurs revendications territoriales en contrôlant le flux de données ou en nuisant à des réparations cruciales. Les États-Unis et leurs alliés mettent en garde contre le risque d'espionnage, de cyberattaques et de surveillance de la part de la Chine et encouragent les pays de l'ASEAN à diversifier leurs partenaires commerciaux en ce qui concerne les câbles. Toutefois, les pays de la région ne sont pas davantage à l'abri de tels risques venant des États-Unis et de leurs alliés.[194] Ainsi, les pays de l'ASEAN sont confrontés à de plus en plus de pressions pour choisir entre le camp occidental, composé des États-Unis et de leurs alliés, et le camp chinois. Ceci ne contribue pas à renforcer la résilience du réseau et la gouvernance numérique régionale. Les câbles sous-marins sont mêlés aux enjeux géopolitiques en MCM et à la concurrence en Indo-Pacifique, freinant ainsi les bénéfices que la démocratisation de la connexion Internet procure à l'Asie du Sud-Est.[195] Les câbles sous-marins sont un autre outil pour la Chine d'exercer une pression sur les

[192] Desurmont, J.-M., *Op. cit.*
[193] Kang, J. et Jacob, J., *Op. cit.*, p. 9.
[194] Desurmont, J.-M., *Op. cit.*
[195] *Ibid.*

États afin de les amener à accepter ses revendications territoriales. Cette stratégie s'inscrit dans la zone grise, l'intention de la Chine n'étant pas explicite.

De plus, entre 2019 et 2023, il y aurait eu 36 cas de dommages subis par les câbles de Taïwan et causés par des forces externes. La cause principale serait les ancres des bateaux. En 2025, Taïwan a signalé, pour l'instant, cinq cas de dommages portés aux câbles sous-marins. Si ces dommages ne sont pas attribuables à un sabotage orchestré par la Chine contre Taïwan, les incidents coïncident avec l'intensification des mesures adoptées par Pékin contre Taipei, qu'il s'agisse d'exercices militaires, d'intrusions dans l'espace maritime taïwanais ou encore de cyberattaques contre les infrastructures critiques de l'île.[196] Les câbles sous-marins sont désormais au cœur des enjeux stratégiques de la région, servant d'instruments de la zone grise, mais aussi de nouveau terrain de la compétition technologique sino-américaine. Les cas taïwanais permettent d'illustrer ces tendances émergentes. En résumé, la compétition entre les États-Unis et la Chine entraîne une fragmentation du réseau de câbles, ce qui augmente la pression sur les nations d'Asie du Sud-Est et de MCM à choisir un camp, à choisir entre les infrastructures fournies par la Chine ou bien celles fournies par les États-Unis et leurs alliés.[197] Par sa stratégie de découplage, Washington a tenté de dissuader les acteurs de la région de passer des contrats avec des câblo-opérateurs chinois, tels que HMN Tech, en raison du risque d'espionnage et de transfert forcé de données. Cependant, les pays de la région sont confrontés aux mêmes risques de la part des États-Unis.[198] Par ses actions en zone grise, la Chine teste les limites de Taïwan et de ses alliés, tout en restant sous le seuil d'une confrontation conventionnelle.[199] Les câbles sont donc utilisés comme des vecteurs d'influence et de menace, tout en étant considérés comme des infrastructures critiques à protéger.

---

[196] Insikt Group. (2025, 17 juillet). *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity* [Threat Analysis]. Insikt Group. <https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats>, p. 10-11.

[197] Noor, E. (2024). Entangled: Southeast Asia and the Geopolitics of Undersea Cables. *Indo-Pacific Outlook, 1*(5), 1-10. University of Hawai'i at Mānoa, Center for Indo-Pacific Affairs. <https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables/>, p. 1.

[198] Noor, E., Subsea Communication Cables in Southeast Asia*, Op. cit.*, p. 9.; Desurmont, J.-M., *Op. cit.*

[199] Lee, S.-F. (2024). Decoding Beijing's Gray Zone Tactics: China Coast Guard Activities and the Redefinition of Conflict in the Taiwan Strait. *Global Taiwan Institute, 9*(6), 6-9. <https://globaltaiwan.org/2024/03/decoding-beijings-gray-zone-tactics-china-coast-guard-activities-and-the-redefinition-of-conflict-in-the-taiwan-strait/>, p. 6.

En outre, les routes numériques physiques qui composent le cyberespace se trouvent au centre des stratégies de confrontation. En effet, le contrôle et la défense de ces infrastructures sont aujourd'hui des facteurs clés de la liberté de manœuvre des acteurs civils, politiques et militaires.[200] Dans la conduite des opérations militaires, la maîtrise de ces infrastructures critiques représente un avantage majeur et confère une supériorité informationnelle et technologique. Les câbles sous-marins témoignent également de la capacité de projection de la puissance des États. La maîtrise des routes numériques exprime donc des rapports de force entre puissances ainsi qu'un enjeu stratégique qui devient de plus en plus visible.[201] Les câbles sous-marins de télécommunications se retrouvent de plus en plus au sein des stratégies nationales visant à assurer la supériorité technologique, à l'image de la concurrence numérique sino-américaine. Les câbles font partie de ces technologies à double usage qui se trouvent en zone grise et qui présentent un caractère hybride, à la fois civil et militaire. Leur hybridité réfère également aux divers domaines qui sont concernés, à savoir leur aspect physique ainsi que leur aspect digital et informationnel. Étant vulnérables, leur protection est essentielle afin d'assurer la sécurité nationale et garantir la circulation de l'information entre les pays et les continents. Les câbles situés en Asie du Sud-Est et en MCM sont particulièrement vulnérables aux tensions régionales, comme le montre le cas de Taïwan. Ainsi, plusieurs stratégies sont mises en place pour sécuriser les câbles, comme le renforcement des liens entre les secteurs public et privé, la stratégie de découplage ou encore la stratégie d'évitement. Les quelques stratégies de sécurisation nommées ne sont évidemment pas exhaustives, mais leur étude permet de montrer les tendances majeures. Les câbles sont non seulement considérés comme des infrastructures essentielles qui doivent être protégées par des stratégies de sécurisation, mais également comme des instruments au service d'une stratégie nationale de confrontation, révélant par le fait même les rapports de force.

[200] Namor, A., *Op. cit.*, p. 102.
[201] *Ibid.*, p. 96.

CONCLUSION

Les fonds marins sont de plus en plus le théâtre de la concurrence technologique entre les puissances, ce qui souligne la nécessité d'étudier les stratégies de sécurisation des câbles sous-marins. L'accès à l'information et la supériorité technologique sont en effet des enjeux stratégiques, et les câbles sont des outils au service de ces intérêts nationaux. À travers une synthèse des connaissances, ce travail vise à mieux comprendre la manière dont les États d'Asie du Sud-Est et de la MCM réagissent lorsque des actes de sabotage visent leurs câbles sous-marins, en particulier lorsqu'un acteur étatique est soupçonné d'en être à l'origine. L'étude se concentre sur les actions directes, c'est-à-dire les incidents affectant le réseau physique de câbles, et non sur l'information transmise par ces câbles. L'analyse se concentre sur le cas de Taïwan en posant la question suivante : comment est-ce que Taïwan réagit face au sabotage intentionnel de ses câbles sous-marins par la Chine ? En répondant à cette question, le travail contribue à combler certaines lacunes identifiées par la littérature, à savoir le manque d'attention académique portée aux dommages intentionnels orchestrés par un État ainsi qu'aux réactions des États visés. Le travail a également permis d'étudier comment les méthodes en zone grise, les dynamiques de pouvoir et la concurrence numérique sino-américaine se manifestent dans le cas des câbles sous-marins à Taïwan, mais aussi en Asie du Sud-Est et en MCM de manière plus générale. En raison de la difficulté d'attribution et des méthodes en zone grise, les cas confirmés sont peu nombreux. C'est pourquoi les cas de Taïwan ont été particulièrement étudiés, malgré le statut particulier de l'île. En effet, Taïwan n'est pas reconnu comme un État souverain sur la scène internationale, mais bénéficie tout de même d'une certaine indépendance politique.

Les risques et les menaces qui pèsent sur les câbles sous-marins montrent la vulnérabilité de ces infrastructures critiques et essentielles à la circulation mondiale des données Internet. Leur importance stratégique reflète également l'intérêt de les prendre pour cible afin de nuire et perturber les télécommunications de certains États. Si l'intérêt stratégique de ces câbles est reconnu en Asie du Sud-Est et en MCM, peu d'études académiques se penchent sur le sujet et encore moins traitent des attaques volontaires contre ces infrastructures. En effet, s'ils sont reconnus comme des infrastructures critiques et stratégiques, les câbles à fibre optique sont rarement étudiés comme objet central des recherches en études stratégiques ou en science politique. Ces lacunes deviennent

particulièrement apparentes lorsque des incidents visant ces câbles surviennent, comme c'est le cas à Taïwan, car elles entraînent une méconnaissance du sujet. À l'invisibilité des câbles s'ajoutent la multitude d'acteurs et le caractère interdépendant du réseau qui complexifient l'enjeu. Les méthodes d'attaques en zone grise rendent l'attribution et la classification des attaques plus difficiles, limitant ainsi les cas confirmés d'attaques intentionnelles.

En outre, malgré l'interdépendance du réseau câblé, la continuité des dynamiques de pouvoir transparaît par la compétition technologique stratégique entre la Chine et les États-Unis. La présente recherche conclut que le cas des câbles sous-marins en Asie du Sud-Est et en MCM s'inscrit dans la rivalité numérique sino-américaine dans cette région, illustrant ainsi les tensions et les rapports de force préexistants sur la scène internationale. Le cas de Taïwan montre que les câbles sont désormais perçus non seulement comme des infrastructures critiques devant être protégées contre des menaces extérieures, mais également comme des vecteurs d'influence et de menace. Les deux premières puissances économiques mondiales participent à une course à la supériorité technologique et le secteur des câbles sous-marins n'y fait pas exception. Washington et Pékin tentent tous deux d'étendre leur influence dans le secteur câblé en Asie du Sud-Est et en MCM. De plus, le travail met en lumière des actes qui s'inscrivent dans le cadre des méthodes en zone grise, révélant ainsi une tendance émergente quant à l'instrumentalisation des câbles sous-marins de télécommunications dans ce genre de pratiques. La Chine teste les limites de Taïwan et de ses alliés en recourant à des méthodes en zone grise, notamment par l'intermédiaire d'acteurs tiers. Les coupures de câbles survenues à Taïwan en 2023 et 2025 expriment une tendance croissante quant à l'instrumentalisation de ces infrastructures par la Chine pour exercer une pression supplémentaire sur Taïwan. En effet, les câbles sont utilisés par la Chine comme technique de perturbation dirigée contre Taïwan afin d'imposer sa volonté de manière indirecte et sans recourir à la force cinétique. Ainsi, la zone grise concernant les câbles sous-marins semble s'assombrir et devenir de plus en plus opaque, l'enjeu de l'attribution constituant un obstacle clair à l'identification des incidents. Les États-Unis, quant à eux, étendent leur influence dans le domaine des câbles et dans la région en participant à de nombreux projets câblés, notamment avec Taïwan. Les États-Unis poursuivent également leur stratégie de découplage en séparant au maximum les réseaux câblés américains de ceux chinois, alimentant ainsi les tensions dans la région. L'exemple de Taïwan révèle la continuité de la compétition technologique et stratégique entre les États-Unis

et la Chine, ainsi que l'émergence de techniques en zone grise visant les câbles sous-marins. Ces tendances reflètent la perception des câbles comme des outils d'influence et de menace, en plus d'être des infrastructures critiques à protéger.

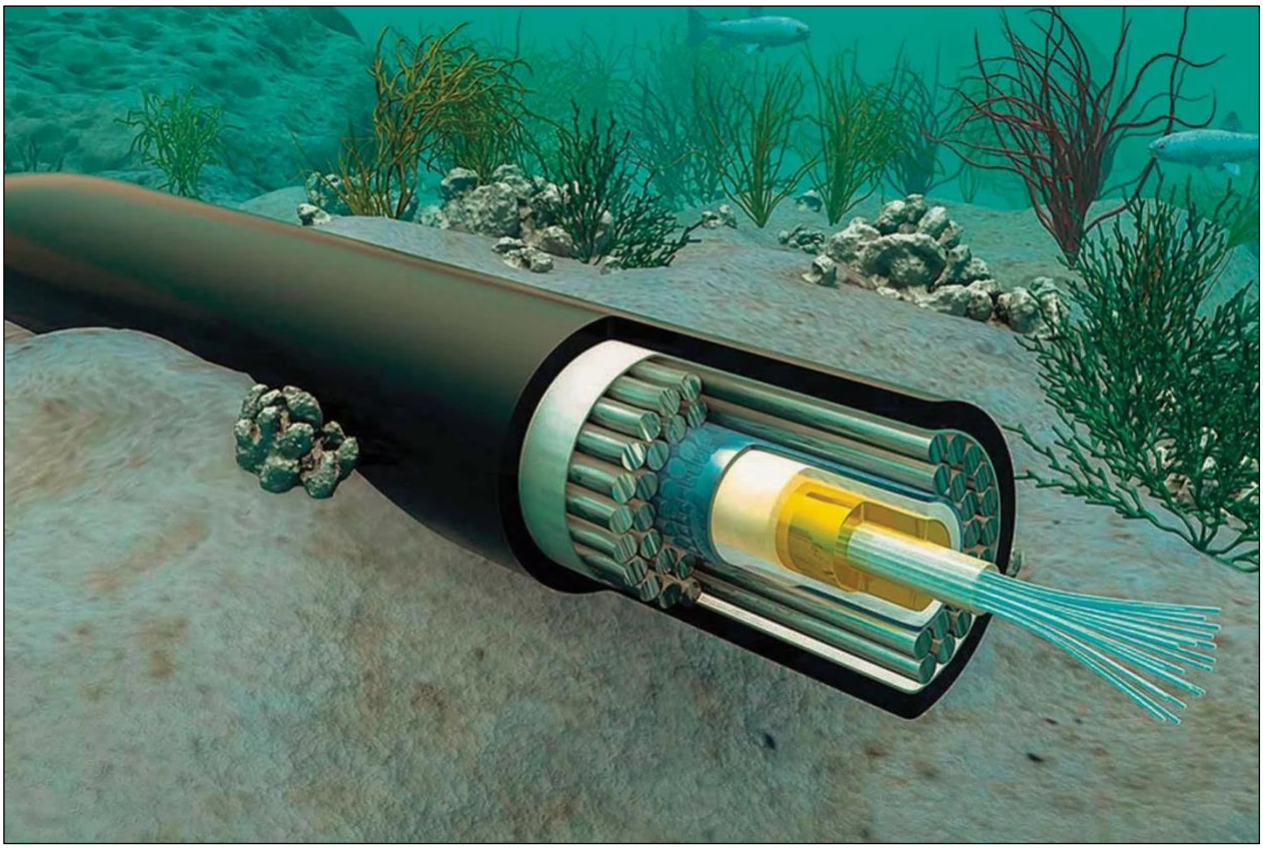
Taïwan se retrouve au cœur de ces tensions géopolitiques, notamment en raison de son importance stratégique pour les grandes puissances. Ainsi, les rapports de force dans le domaine câblé se manifestent également dans le cas de Taïwan. Taipei a mis en œuvre plusieurs stratégies de sécurisation en réponse aux incidents étudiés, telles que la reconnaissance des câbles sous-marins comme infrastructures critiques, le renforcement du cadre juridique, la coopération bilatérale avec des alliés, le renforcement de sa stratégie de défense par le biais d'un financement accru de la garde côtière taïwanaise, ainsi que la mise en œuvre de nouveaux projets de câbles, ce qui permet d'augmenter la redondance du réseau. Ces stratégies de sécurisation peuvent servir d'exemple aux États qui sont confrontés ou qui pourraient être confrontés à des enjeux similaires à l'avenir, dans un contexte international où la supériorité technologique et le contrôle de l'information sont des enjeux stratégiques.

Alors que les incidents affectant les câbles sous-marins deviennent de plus en plus fréquents, les formes superposées d'invisibilité et les méthodes en zone grise rendent l'étude de ces câbles particulièrement complexe, soulignant ainsi la nécessité d'approfondir le sujet. Le manque de cas confirmés et la confidentialité du sujet constituent d'ailleurs les principales limites du présent travail de recherche. S'il existe peu de cas confirmés d'attaques volontaires directes de la part d'un État contre des câbles, une tendance émergente semble prévoir une augmentation de ce genre d'incidents à l'avenir, dans le cadre des méthodes en zone grise. De plus, malgré leurs multiples formes d'invisibilité, les câbles sous-marins figurent parmi les technologies qui caractérisent la concurrence numérique sino-américaine. La sécurisation des câbles est complexe en raison de l'interconnexion multinationale des réseaux, qui implique de nombreux acteurs étatiques et privés, ainsi que plusieurs législations. La classification des dommages potentiellement intentionnels subis par les câbles reste ardue, notamment en raison des méthodes en zone grise. Le présent travail encourage l'étude des stratégies de sécurisation en réponse aux incidents volontaires visant les câbles afin de rendre cet enjeu stratégique plus visible. Outre les acteurs étatiques, une attention particulière devrait être portée envers les groupes terroristes et les réseaux criminels afin de

déterminer leurs intentions, leurs moyens d'action et le soutien potentiel qu'ils reçoivent d'un acteur étatique. Ce sujet pourrait faire l'objet de futures recherches afin d'étudier les tendances émergentes relatives aux acteurs non étatiques dans le domaine câblé. Une étude comparative serait également pertinente. Puisque le nombre d'atteintes intentionnelles confirmées et commises par un État dans une même région est limité, une comparaison pourrait porter sur des incidents survenus dans des régions différentes du monde. Une autre comparaison pourrait étudier les mesures mises en œuvre par deux États en réaction au sabotage perpétré par un même État tiers. La comparaison des stratégies de sécurisation des câbles sous-marins présente des pistes pertinentes pour de futures recherches.

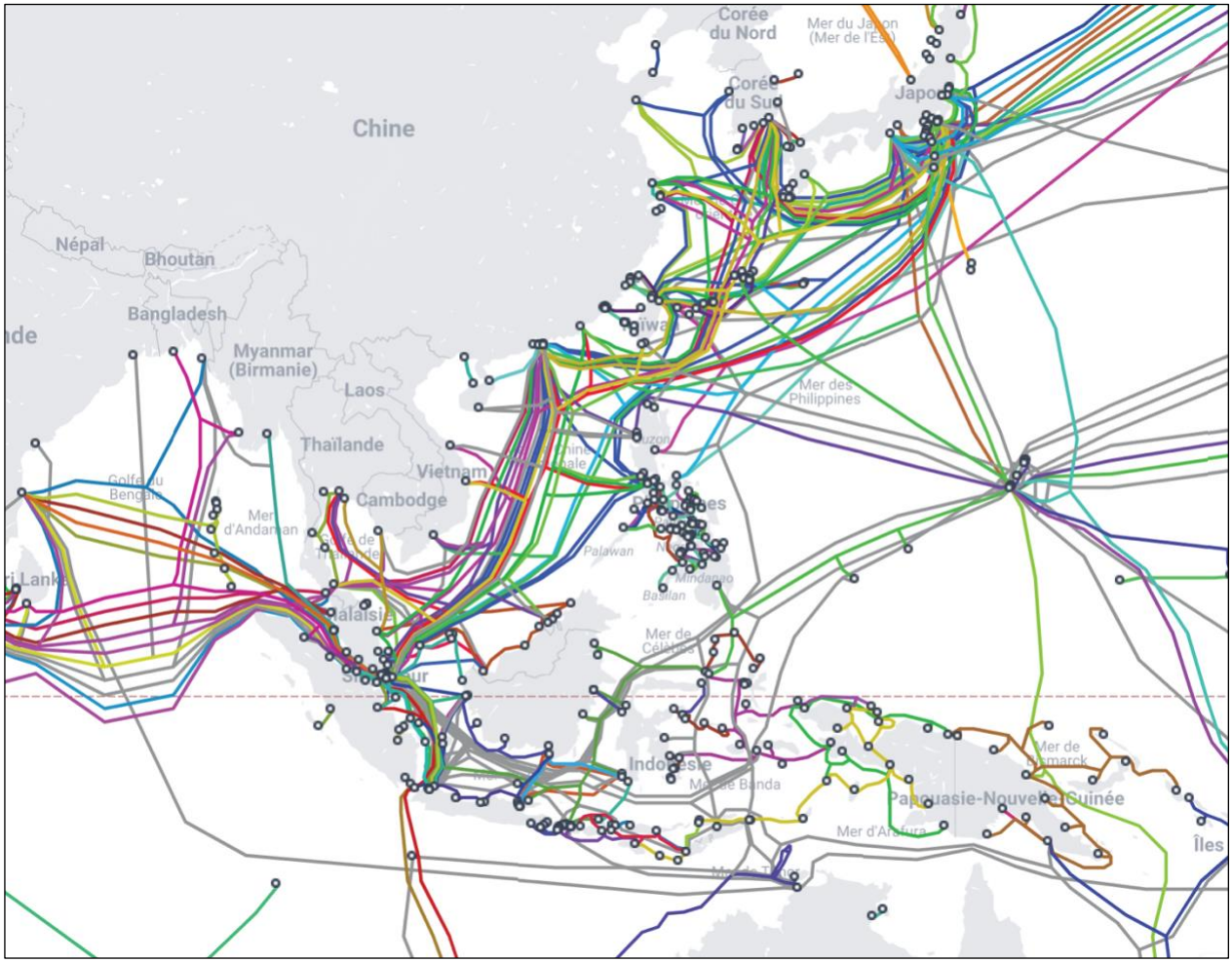
ANNEXES

Figure 1. Illustration d'un câble sous-marin



Source : Quốc Tế, B. (2024, 29 décembre). Câble optique - Système d'armes sous-marines stratégiques. *Vietnam.vn*. <https://www.vietnam.vn/fr/cap-quang-he-vu-khi-chien-luoc-duoi-long-bien>.

Figure 2. Carte des câbles sous-marins en Asie du Sud-Est et en mer de Chine méridionale



Source : TeleGeography, *Submarine Cable Map*, <https://www.submarinecablemap.com/>.

BIBLIOGRAPHIE

Annathurai, R. M. (2023). *Battles below: Submarine Cables in Naval Warfare and International Humanitarian Law*. Symposium Maritime Operations and Humanitarian Considerations. <https://www.researchgate.net/publication/377629871_BATTLES_BELOW_SUBMARINE_CABLES_IN_NAVAL_WARFARE_AND_INTERNATIONAL_HUMANITARIAN_LAW_Session_1_International_Humanitarian_Law_Naval_Operations>.

ASEAN Secretariat. (2025). *About us*. ASEAN Main Portal. <https://asean.org/about-us/>.

Bastien-Carignan, N., Girard, P. et Lecchino, M. (2025, 14 juillet). Débranchez Taïwan, et le monde s'éteint. *Le Devoir*. <https://www.ledevoir.com/opinion/idees/900046/idees-debranchez-taiwan-monde-eteint>.

Baum, A., Salgame, N. et Zolyniak, A. (2025, 11 février). Water Wars: Trump, Taiwan, and the Philippines. *The Lawfare Institute*. <https://www.lawfaremedia.org/article/water-wars--trump--taiwan--and-the-philippines>.

Beckman, R. (2014). Chapter 12. Protecting Submarine Cables from Intentional Damage – The Security Gap. Dans D. R. Burnett, R. Beckman et T. M. Davenport (dir.), *Submarine Cables - The Handbook of Law and Policy* (p. 281-297). Brill. <https://doi.org/10.1163/9789004260337_014>.

Beyer, J. L. *et al*. (2025). *Hidden Highways of the Internet: Global Subsea Cable Security* [Task Force Report]. Henry M. Jackson School of International Studies, University of Washington. <https://jsis.washington.edu/wordpress/wp-content/uploads/2025/03/Task-Force-B-Final-Report.pdf>.

Botting, A. et Jordan-Zoob, I. (2024, 28 février). Optical Core Infrastructure: The Hidden Highway of Connectivity. *Wilson Center*. <https://www.wilsoncenter.org/article/optical-core-infrastructure-hidden-highway-connectivity>.

Brake, D. (2019). Submarine Cables: Critical Infrastructure for Global Communications. *Information Technology and Innovation Foundation (ITIF)*, 1-11. <https://www2.itif.org/2019-submarine-cables.pdf>.

Brock, J. (2023, 24 mars). U.S. and China wage war beneath the waves - over internet cables. *Reuters* (Singapore). <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>.

Bueger, C. et 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>.

Burdette, L. (2024, 21 novembre). *What To Know About Submarine Cable Breaks*. TeleGeography. <https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks>.

Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Boulder, Colorado: L. Rienner, 2nd ed.

Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium, 43*(2), 640-659. <https://doi.org/10.1177/0305829814562655>.

Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists, 72*(4), 234-237. <https://doi.org/10.1080/00963402.2016.1195636>.

Connatser, M. (2024, 18 juin). Vietnam's internet again in trouble as three of five submarine cables go down. *The Register*. <https://www.theregister.com/2024/06/18/vietnam_internet_cables/>.

Desurmont, J.-M. (2024, 21 mai). *Territorial Claims and Subsea Cables: The Geopolitics of Invisible Lines in the South China Sea*. Bloomsbury Intelligence & Security Institute (BISI). <https://bisi.org.uk/reports/territorial-claims-and-subsea-cables-the-geopolitics-of-invisible-lines-in-the-south-china-sea>.

Detry, C.-E. (2023). *La résolution 2758 de l'AGNU et le statut de Taïwan en droit international*. Fondation pour la Recherche Stratégique (FRS). <https://www.frstrategie.org/sites/default/files/documents/programmes/Programme-Taiwan/2023/01-2023.pdf>.

Eurasia Group. (2020). *The Geopolitics of Semiconductors*. <https://www.eurasiagroup.net/live-post/geopolitics-semiconductors>.

Fernandes, C. (2021). Subterranean statecraft: Invisible diplomacy in Australia's external relations. *Geoforum, 127*, 385-389. <https://doi.org/10.1016/j.geoforum.2020.02.007>.

Ganz, A. *et al*. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines, 34*(31), 1-23. <https://doi.org/10.1007/s11023-024-09683-z>.

Goldrick, J. (2018). *Grey Zone Operations and the Maritime Domain* [Special report]. Australian Strategic Policy Institute (ASPI). <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ASPI_SR%20131%20Grey%20zone%20operations.pdf>.

Government of Timor-Leste. (2024, 25 juin). *Government Carries Out First Submarine Fiber Optic Cable Installation*. <https://timor-leste.gov.tl/?p=38073&lang=en&n=1>.

Greene, R. et Triolo, P. (2020, 8 mai). Will China Control the Global Internet Via its Digital Silk Road? *Carnegie Endowment for International Peace & SupChina*. <https://carnegieendowment.org/posts/2020/05/will-china-control-the-global-internet-via-its-digital-silk-road?lang=en>.

Harding, B. (2019, 15 février). China's Digital Silk Road and Southeast Asia. *Center for Strategic and International Studies (CSIS)*. <https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia>.

Indo-Pacific Defense FORUM. (2025, 28 septembre). Taiwan strengthens patrols against China's undersea cable sabotage. *Indo-Pacific Defense FORUM*. <https://ipdefenseforum.com/2025/09/taiwan-strengthens-patrols-against-chinas-undersea-cable-sabotage/>.

Insikt Group. (2025, 17 juillet). *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity* [Threat Analysis]. Insikt Group. <https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats>.

Kang, J. et Jacob, J. (2024). *Connecting the Indo-Pacific: The future of subsea cables and opportunities for Australia*. Australian Strategic Policy Institute (ASPI). <https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/>.

Kim, J., Kim, H. et Terasawa, M. (2025, 16 mai). The World's Subsea Cables Are Under Threat. Can Canada Help Protect Them? *Asia Pacific Foundation of Canada*. <https://www.asiapacific.ca/fr/publication/les-cables-sous-marins-du-monde-entier-sont-menaces-le>.

Lee, S.-F. (2024). Decoding Beijing's Gray Zone Tactics: China Coast Guard Activities and the Redefinition of Conflict in the Taiwan Strait. *Global Taiwan Institute, 9*(6), 6-9. <https://globaltaiwan.org/2024/03/decoding-beijings-gray-zone-tactics-china-coast-guard-activities-and-the-redefinition-of-conflict-in-the-taiwan-strait/>.

Leymarie, P. (2022, 1er mars). Le club des « cinq » face à la Chine. *Le Monde diplomatique*, p. 11. <https://www.monde-diplomatique.fr/2022/03/LEYMARIE/64415>.

Linh, T. (2017, 29 août). Internet : trois câbles sous-marins du Vietnam endommagés. *Le Courrier du Vietnam*. <https://lecourrier.vn/internet-trois-cables-sous-marins-du-vietnam-endommages/424355.html>.

Marine & Océans. (2025, 12 juin). Taïwan : un capitaine chinois emprisonné pour avoir sectionné un câble sous-marin. *Marine & Océans* (Taipei). <https://marine-oceans.com/actualites/taiwan-un-capitaine-chinois-emprisonne-pour-avoir-sectionne-un-cable-sous-marin/>.

McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. *Australian Journal of International Affairs, 76*(2), 161-177. <https://doi.org/10.1080/10357718.2022.2051427>.

Morel, C. (2023). L'Asie du Sud-Est, nouveau centre de gravité des câbles sous-marins. Dans *L'Asie du Sud-Est 2023 : bilan, enjeux et perspectives* (p. 73-109). Institut de recherche sur l'Asie du Sud-Est contemporaine (IRASEC). <https://doi.org/10.4000/books.irasec.6391>.

Morel, C. (2021). Sous la mer, le monde numérique : Une géopolitique des câbles sous-marins. *Questions internationales, 1*(107-108), 81-87. <https://doi.org/10.3917/quin.107.0081>.

Morel, C. (2019). La mise en péril du réseau sous-marin international de communication. *Flux, 118*(4), 34-45. <https://doi.org/10.3917/flux1.118.0034>.

Morel, C. (2018). Protéger nos infrastructures vitales pour assurer notre résilience : les câbles sous-marins, entre invisibilité et vulnérabilité. *Les Champs de Mars, 30*(1), 419-426. <https://doi.org/10.3917/lcdm.030.0419>.

Morel, C. (2017). Les câbles sous-marins : un bien commun mondial ? *Études*, (3), 19-28. <https://doi.org/10.3917/etu.4236.0019>.

Morel, C. (2016). Menace sous les mers : les vulnérabilités du système câblier mondial. *Hérodote, 163*(4), 33-43. <https://doi.org/10.3917/her.163.0033>.

Morel, C. (2015). Stratégie maritime – Le réseau mondial de câbles sous-marins : une toile dans la Toile. *Revue Défense Nationale, 784*(9), 117-120. <https://doi.org/10.3917/rdna.784.0117>.

Namor, A. (2022). La conquête des routes numériques. *Inflexions, 49*(1), 95-102. <https://doi.org/10.3917/infle.049.0095>.

Noor, E. (2024). Entangled: Southeast Asia and the Geopolitics of Undersea Cables. *Indo-Pacific Outlook, 1*(5), 1-10. University of Hawai'i at Mānoa, Center for Indo-Pacific Affairs. <https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables/>.

Noor, E. (2024). Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables?lang=en>.

Ocon, J. et Walberg, J. (2025). China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities. *Global Taiwan Institute, 10*(11), 9-12. <https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/>.

Photonics. (2007, 8 juin). Cable Theft Costs Vietnam $6M. *Photonics* (Ho Chi Minh, Vietnam). <https://www.photonics.com/Articles/Cable_Theft_Costs_Vietnam_6M/a29904>.

Quốc Tế, B. (2024, 29 décembre). Câble optique - Système d'armes sous-marines stratégiques. *Vietnam.vn*. <https://www.vietnam.vn/fr/cap-quang-he-vu-khi-chien-luoc-duoi-long-bien>.

Racho, T. (2022). Les câbles sous-marins, des infrastructures internet critiques. *La revue européenne des médias et du numérique*, (61-62). <https://la-rem.eu/2022/10/les-cables-sous-marins-des-infrastructures-internet-critiques/>.

RFI. (2025, 11 avril). Taïwan : un capitaine chinois inculpé pour avoir coupé un câble sous-marin essentiel pour l'île. *RFI (Radio France Internationale)*, Asie-Pacifique. <https://www.rfi.fr/fr/asie-pacifique/20250411-ta%C3%AFwan-un-capitaine-chinois-inculp%C3%A9-pour-avoir-coup%C3%A9-un-c%C3%A2ble-sous-marin-essentiel-pour-l-%C3%AEle>.

Rinaldi, T. (2025, 10 septembre). Taiwan advances undersea cable defense strategy. *Taiwan News* (Taipei). <https://taiwannews.com.tw/en/news/6197737>.

Roach, J. A. (2014). Chapter 15. Military Cables. Dans D. R. Burnett, R. Beckman et T. M. Davenport (dir.), *Submarine Cables - The Handbook of Law and Policy* (p. 339-349). Brill. <https://doi.org/10.1163/9789004260337_017>.

Ross, M. (2014). Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security. *SAIS Review of International Affairs, 34*(1), 141-155. <https://muse.jhu.edu/pub/1/article/547670>.

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). *Marine Policy, 171*(106434). <https://doi.org/10.1016/j.marpol.2024.106434>.

Rozel, B. (2009). La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances. Thèse, Institut polytechnique de Grenoble.

Starosielski, N. (2015). Circuitous Routes: From Topology to Topography. Dans *The Undersea Network* (1ère éd., p. 26-63). Durham, États-Unis: Duke University Press. <http://ebookcentral.proquest.com/lib/uqam/detail.action?docID=1974178>.

Swinhoe, D. (2021, 26 août). What is a submarine cable? Subsea fiber explained. *Data Centre Dynamics (DCD)*. <https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/>.

TeleGeography. (s.d.). *Submarine Cable Map*. <https://www.submarinecablemap.com/>.

The Australian Infrastructure Financing Facility for the Pacific (AIFFP). (s.d.). *Connecting Timor-Leste to the internet via submarine cable*. <https://www.aiffp.gov.au/investments/investment-list/connecting-timor-leste-to-the-internet-via-submarine-cable>.

Tzu-ti, H. (2025, 19 septembre). Taiwan proposes tougher laws to protect undersea cables. *Taiwan News* (Taipei). <https://taiwannews.com.tw/en/news/6203736>.

Winseck, D. (2017). The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy, 7*, 228-267. <https://doi.org/10.5325/jinfopoli.7.2017.0228>.