# MENACE SOUS LES MERS : LES VULNÉRABILITÉS DU SYSTÈME CÂBLIER MONDIAL

Camille Morel

La Découverte | « Hérodote »

2016/4 N° 163 | pages 33 à 43

ISSN 0338-487X
ISBN 9782707192295

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-herodote-2016-4-page-33.htm

Pour citer cet article :

Camille Morel, « Menace sous les mers : les vulnérabilités du système câblier mondial », *Hérodote* 2016/4 (N° 163), p. 33-43.
DOI 10.3917/her.163.0033

# Menace sous les mers : les vulnérabilités du système câblier mondial

*Camille Morel*[1]

L'attaque d'un navire câblier par des pirates en mer Rouge à l'été 2016 a confirmé des hypothèses jusque-là non avérées. En pleine opération de pose d'un câble sous-marin, le navire s'est retrouvé cerné par les tirs des assaillants, avant de parvenir, finalement, à repousser l'adversaire... Une action malveillante significative contre le système câblier en mer qui vient donner un sens à des années de prospective. Contrairement aux postulats émis et aux faits déjà rencontrés, ce n'est pas l'infrastructure câblière proprement dite qui a été visée, mais le bâtiment en mer responsable des opérations, alors en position vulnérable. Plusieurs faits laissaient déjà présager un tel phénomène depuis quelques années. Mais que vient remettre en cause cette nouvelle attaque ? Doit-on s'inquiéter davantage qu'auparavant de l'intégrité physique du système câblier et de ses acteurs ?

Au service des télécommunications et du Web, les fils de fibre optique apparaissent désormais comme les vecteurs principaux d'une économie mondiale devenue largement connectée. C'est en effet à travers les profondeurs marines que l'information alimente la Toile, transmise à 99 % par le réseau sous-marin. Liaison par excellence entre les univers numérique et maritime, cette infrastructure joue un rôle primordial dans le transfert des données. Finance, commerces en tout genre, administrations et armées utilisent aujourd'hui ce mode de transmission. Les conséquences d'une rupture de câble sont donc importantes. Le réseau militaire de communication de l'US Navy, le Netwarcom, a ainsi été fortement affecté par

1. Doctorante au Centre lyonnais d'études de sécurité internationale et de défense (CLESID), soutenue par la Direction générale des relations internationales et de la stratégie (DGRIS) et l'Institut de recherche stratégique de l'École militaire (IRSEM).

la rupture du câble SEA-ME-WE-3, en 2013[2]. En termes de perte de connectivité et de perte financière, les chiffres parlent d'eux-mêmes. En 2005, L'International Cable Protection Committee[3] (ICPC) évaluait déjà, mais de manière sous-estimée, à 1,5 million de dollars par heure l'impact financier d'une coupure du réseau sous-marin [Matis, 2012, p. 3]. Aujourd'hui, l'ampleur du phénomène s'est accrue, principalement en raison d'une technologie toujours plus consommatrice en données – présence de vidéos sur les réseaux sociaux, utilisation du stockage en ligne, etc.

D'autant plus qu'à cette mission cruciale de transmission des télécommunications s'ajoute celle du transport d'énergie. Les câbles permettent en effet d'alimenter en électricité des îles isolées – comme Belle-Île-en-Mer ou Daydream Island dans l'océan Pacifique – mais aussi de raccorder des éoliennes *offshore* et d'acheminer l'énergie produite vers les centres de traitement. Ces deux fonctions principales rendent les câbles sous-marins vitaux en tout point, et font de ce réseau une cible stratégique potentielle pour des États ou des acteurs non étatiques.

Mais quelles sont aujourd'hui les vulnérabilités du réseau sous-marin et les menaces réelles qui pèsent sur lui ? Si l'activité maritime croissante et les spécificités physiques du milieu marin ont toujours été sources de risques pour cette infrastructure, la mer et les océans comptent désormais parmi les grandes victimes des cyberattaques. Le réseau câblier, étroitement relié au cyberespace, est donc susceptible de subir, lui aussi, ce fléau. Doit-on s'inquiéter de la protection du système de gestion et de contrôle du réseau sous-marin, en grande partie informatisé ? Le statut d'« infrastructure critique », que l'on peut attribuer aux câbles sous-marins en raison de leur fonction, laisse à penser que la menace cyber est en effet latente pour ce système. Une étude comparative portant sur les vulnérabilités des réseaux terrestres de même fonction – transport d'énergie ou de télécommunications – pourrait alors permettre de dessiner quelques hypothèses de menaces, physiques ou cyber, applicables au réseau sous-marin. L'étude des coupures recensées à ce jour sur le système câblier sera finalement instructive. Qu'il s'agisse d'espionnage, de sabotage ou de piraterie, une vue d'ensemble des cas connus permettrait de dresser un bilan des vulnérabilités actuelles et des tendances pour l'avenir.

## ***Deep waters* et cyberattaques**

L'océan dans lequel sont déroulés les câbles sous-marins, vaste et mal maîtrisé, a toujours représenté une menace pour la préservation des lignes en profondeur.

2. Observatoire du monde cybernétique, Délégation aux affaires stratégiques, *Note du 1er trimestre*, mars 2014, p. 23.

3. L'ICPC est l'autorité internationale chargée des questions relatives à la sécurité et à la protection des câbles sous-marins.

Les caractéristiques du milieu marin et son exploitation par l'homme ont en effet créé un cadre hostile au maintien en état de cette infrastructure. Corrosion ou séismes, ancres de navires ou filets de pêche sont autant de causes fréquentes – naturelles ou accidentelles – d'usure ou de rupture de câbles depuis leur origine. Dès 1884, la première convention internationale portant sur la protection du réseau sous-marin cherche ainsi à encadrer le déroulement des activités concurrentes de l'espace maritime. Grâce à cette réglementation, qui intervient moins de trente ans après la mise en service du premier câble télégraphique, les navires ont l'obligation de se tenir à une certaine distance des bâtiments chargés de la pose ou de la maintenance des câbles, afin d'éviter toute détérioration accidentelle. Malgré les prémices d'une régulation, la menace ne faiblit pas : en 2006, près de 90 % du total des perturbations reconnues étaient causées par les cas d'ancrage et les filets de pêche [Salvador *et al.*, p 316]. Et des incidents récents prouvent la persistance de ce risque, notamment au niveau de points névralgiques où la concentration des câbles est maximale et l'activité maritime intense – canal de Suez, détroit de Luçon... L'International Cable Protection Committee, organisme qui tente depuis 1958 de promouvoir la protection de ce réseau, notamment auprès des autres utilisateurs des fonds marins, joue un rôle majeur aujourd'hui encore dans l'effort de sécurisation du système et de diminution des incidents.

Mais une autre dimension remue également les *deep waters* de l'océan. Celle du cyberespace. Le champ lexical d'Internet, intrinsèquement lié au monde maritime, laissait présager cette rencontre : on « surfe » sur le Web, on se connecte grâce à des « logiciels de navigation », des « pirates » s'introduisent sur la Toile... Mais le parallèle entre les deux mondes – le cyber d'un côté, la mer de l'autre – ne s'arrête pas là. Les deux milieux partagent des caractéristiques géographiques essentielles, dont leur immensité et leur ouverture sur le monde [Jacob, 2000, p. 2]. Espaces sans frontières reliant les continents entre eux, ils ont un même atout : unifier le monde en servant de transit entre les terres et les peuples. Chacun contribue également à une mondialisation économique et humaine croissante[4]. Mais l'univers maritime connaît désormais le revers de cette liaison étroite, avec l'apparition d'une autre forme de menace : les cyberattaques.

L'automatisation et l'informatisation des systèmes à grande échelle dans le milieu maritime – phénomène appelé *marétique* – a ouvert de nouvelles fenêtres aux individus malintentionnés[5]. Risques en mer pesant sur les navires comme

4. Si le transport maritime a su révolutionner les échanges et les délais de livraison au cours du XX^e siècle, Internet, lui, est devenu au XXI^e l'outil indispensable d'une nouvelle ère toujours plus connectée.

5. Observatoire du monde cybernétique, Délégation aux affaires stratégiques, *Note du 1^er trimestre*, mars 2014, p. 17.

sur terre dans la gestion des infrastructures portuaires, la diversité des attaques connues à ce jour ne cesse de s'élargir. L'interconnexion et le besoin permanent de systèmes de régulation et de navigation accroissent jour après jour la vulnérabilité des infrastructures maritimes face au risque cyber. Des exemples récents de piratage sur des prototypes d'hydrolienne ou de plateforme *offshore* montrent à quel point la pénétration informatique des systèmes met à mal la sécurité des activités en mer. L'hydrolienne quimpéroise *Sabella*, immergée au large d'Ouessant, a ainsi été prise pour cible par des pirates informatiques en octobre 2015, provoquant une interruption de sa production en électricité pendant plus d'une semaine. Ce cas notable ouvre la voie aux futurs piratages d'infrastructures maritimes. Les câbles sous-marins pourraient donc également subir ce fléau, en tant que couche matérielle du cyberespace. Le manque de protection de l'aspect *hardware* du cyber est une lacune évidente qui se joue au détriment de la sécurisation du réseau sous-marin [Sechrist, 2010, p 41]. Mais la vulnérabilité des câbles sous-marins, reliée à leur double liaison avec le cyberespace et le monde maritime, est également imputable à leur fonction.

## Une cible concrète pour atteindre la société : la notion d'infrastructure critique

> « Ainsi, les infrastructures critiques sont les constructions décisives pour notre société. On peut définir simplement les infrastructures critiques 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. Aux États-Unis, la définition est même un peu plus large. Selon le rapport de la commission de protection des infrastructures critiques (Mea97), ces dernières sont les infrastructures qui sont tellement vitales que leur indisponibilité ou destruction aura un impact affaiblissant sur la sécurité nationale ou économique. »
>
> [Rozel, 2009]

Aujourd'hui, le rôle primordial des câbles sous-marins dans le déroulement des opérations commerciales, financières, militaires, administratives ou même individuelles fait de ce réseau, si l'on en croit la définition citée précédemment, une véritable « infrastructure critique ». Cette notion, qui naît dans les années 1990 aux États-Unis, fait référence à l'ensemble des infrastructures essentielles d'un pays [Galland, 2010, p. 10]. Si, en France, la terminologie est légèrement différente



*Hérodote*, n° 163, La Découverte, 4e trimestre 2016.

– on appelle ces établissements, ouvrages ou installations « point d'importance vitale[6] » –, l'objectif est sensiblement le même : répertorier les systèmes fondamentaux pour la société et en analyser les vulnérabilités afin de mieux les protéger. Dès l'origine, on prête à ce type d'infrastructures deux sortes de vulnérabilités potentielles : des menaces physiques et cyber [Galland, 2010, p. 7]. Les faits accréditeront ces analyses et le rythme des cyberattaques sur les infrastructures critiques ne cessera d'ailleurs de s'accélérer. En 2014, les systèmes de contrôle industriel des infrastructures sensibles américaines auraient connu plus de 245 attaques, si l'on en croit les chiffres donnés par l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Permettant de paralyser la société dans son ensemble, l'attaque de telles infrastructures relève d'un intérêt évident pour des individus malintentionnés. Le réseau de télécommunications apparaît d'ailleurs comme une cible particulièrement rentable parmi les infrastructures critiques. Tout système dépend en effet désormais, directement ou indirectement, des infrastructures de l'information [Johnson, 2013]. Les infrastructures critiques (électricité, pétrole, gaz, eau...) sont les premières à s'appuyer sur des équipements électriques et automatisés, eux-mêmes supervisés par des systèmes informatiques dédiés. D'une absence de réseau découle ainsi l'arrêt quasi automatique des circuits financiers, de la distribution d'eau, d'électricité ou encore du fonctionnement des transports. Des systèmes de contrôle et d'acquisition de données (SCADA), qui permettent la collecte et l'analyse efficaces de données pour réaliser un contrôle automatique des équipements, sont, eux aussi, pleinement vulnérables aux attaques cyber. Ils mettent ainsi en danger les infrastructures critiques qu'ils opèrent. Le cas des cyberattaques réalisées à partir de 2009 grâce au célèbre virus *Stuxnet* illustre ce type de risque : le piratage principal découvert, qui visait le système de pilotage de l'infrastructure nucléaire iranienne, a permis d'attirer l'attention sur le risque plus général qui pèse sur les systèmes vitaux d'un pays.

Le fait qu'une défaillance de l'infrastructure de télécommunications[7] puisse automatiquement avoir un impact sur les autres infrastructures vitales renvoie au

6. Un point d'importance vitale est un « établissement, ouvrage ou installation dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ; ou de mettre gravement en cause la santé ou la vie de la population » [Galland, 2010, p. 10].

7. « L'infrastructure de télécommunications a, depuis quelques décennies, évolué en une infrastructure d'information et de communication composée principalement des différents réseaux téléphoniques (filaires et cellulaires) et de l'ensemble des réseaux formant l'Internet » [Rozel, 2009, p. 18].

principe d'interdépendance des réseaux [Galland, 2010, p. 14]. Ce phénomène garantit à tout attaquant potentiel l'efficacité de son action, par répercussion. L'intérêt d'agir sur l'infrastructure câblière de télécommunications est alors maximal pour tout individu malveillant.

## Réseaux terrestres, réseaux sous-marins : quelles analogies ?

Qu'ils soient terrestres ou sous-marins, les câbles servant à la transmission des télécommunications et au transport d'énergie partagent un certain nombre de caractéristiques communes. Observer les vulnérabilités du réseau terrestre de même fonction pourrait ainsi permettre d'anticiper, dans une approche comparative, les risques qui pèsent sur l'infrastructure sous-marine. Les tubes continentaux connaissent régulièrement des sabotages physiques et des piratages informatiques. Les dysfonctionnements du réseau électrique terrestre ukrainien de décembre 2015 a par exemple marqué un tournant en la matière : il s'agit de la première cyberattaque d'une telle ampleur réalisée sur une infrastructure vitale de nature civile, et pouvant compromettre la vie humaine [Siboni et Magen, 2016]. Cet événement sans précédent, vraisemblablement causé par des acteurs liés au gouvernement russe, pourrait servir de modèle à d'autres acteurs, États ou organisations. En termes d'attaque physique, on ne compte plus le nombre de sabotage de lignes de fibre optique et de réseaux d'électricité terrestres. Le cas des pipelines, canalisations servant le transport de fluide et auxquelles sont souvent associés les câbles sous-marins au niveau juridique – notamment par la convention des Nations unies sur le droit de la mer (CNUDM)[8] –, apporte une vision complémentaire des risques pesant sur le réseau sous-marin. La récente attaque d'un oléoduc dans le delta du Niger en mai 2016, réalisé par des rebelles nigérians, prolonge ainsi la longue série d'offensives ayant touché des infrastructures terrestres d'énergie.

Ces différents exemples permettent d'évaluer la vulnérabilité des réseaux terrestres et sensibilisent, par analogie, aux risques potentiels pesant sur l'infrastructure sous-marine. Évidemment, le milieu marin dans lequel évolue le réseau limite

8. Voir notamment l'article 113 portant sur la rupture ou détérioration d'un câble ou d'un pipeline sous-marin : « Tout État adopte les lois et règlements nécessaires pour que constituent des infractions passibles de sanctions la rupture ou la détérioration délibérée ou due à une négligence coupable par un navire battant son pavillon ou une personne relevant de sa juridiction d'un câble à haute tension ou d'un pipeline sous-marin en haute mer, ainsi que d'un câble télégraphique ou téléphonique sous-marin dans la mesure où il risque de s'ensuivre des perturbations ou l'interruption des communications télégraphiques ou téléphoniques. »

considérablement l'accès aux câbles en profondeur et complique donc toute action malveillante. Les contraintes du milieu agissent en effet comme un obstacle et expliquent la faible fréquence des attaques.

Le réseau câblier sous-marin est cependant lui-même composé d'éléments terrestres qui le rendent plus vulnérable. En effet, lorsque les câbles regagnent la surface après leur long séjour sous-marin, ils rejoignent une « station d'atterrissement » sur la côte. Ces bâtiments servent à relier la fibre optique sous-marine au réseau terrestre pour l'acheminement des télécommunications et de l'énergie. Composants « secs » du système, ils sont bien plus accessibles que l'ensemble du réseau immergé, et s'assimilent ainsi à toute autre infrastructure terrestre des réseaux de télécommunications ou d'énergie. Les risques qui pèsent sur l'un pèsent également sur l'autre. Attaque par explosifs ou assauts armés sur le bâtiment, sabotages des équipements ou du générateur d'énergie, offensives indirectes par interruption du courant ou encore piratage des systèmes informatiques sont à craindre [DHS, 2004]. Pour un acteur malveillant, l'intérêt d'une attaque physique sur les stations d'atterrissement est d'ailleurs très grand : ces sites concentrent un nombre important de câbles en leur sein, créant une possibilité de frappe simultanée en une seule attaque. Enfin, les navires servant à la pose et à la maintenance des câbles sont des « bâtiments » assimilables d'une certaine manière à des cibles terrestres. La capacité d'action sur ces éléments semble évidemment plus aisée que sur le reste de l'infrastructure câblière, majoritairement immergée. L'attaque récente du navire câblier par des pirates en mer Rouge, évoquée en introduction, confirme d'ailleurs cette vision de la fragilité du réseau.

## Espionnage, sabotage, piraterie, terrorisme ?

Jusqu'alors les actions malveillantes opérées sur les câbles concernaient seulement le niveau étatique. Les États sont historiquement les seuls à déterminer l'intérêt stratégique du réseau sous-marin, le droit international leur accorde d'ailleurs une liberté d'action sur les câbles sous-marins en temps de guerre. La première coupure volontaire d'un câble sous-marin par un État ennemi s'est déroulée lors du conflit hispano-américain de 1898. À partir de cette date, les actes militaires contre les câbles se généralisent. La Seconde Guerre mondiale démontre d'ailleurs particulièrement l'importance stratégique accordée à la mise en défaut du système. Une des premières actions effectuées par les Alliés au début des hostilités sera ainsi de couper le réseau sous-marin desservant l'Allemagne afin d'isoler l'ennemi. Le renseignement d'État emploie également les câbles sous-marins afin de récolter de l'information. Le réseau Sound Surveillance System (SOSUS), installé en partie depuis des câbles sous-marins par les Américains lors de la

guerre froide, a ainsi servi à espionner l'activité des sous-marins soviétiques en Atlantique. Le milieu aquatique et la profondeur des installations – aussi bien télégraphiques, coaxiales, que de fibre optique – impliquent une importante difficulté d'accès au réseau sous-marin. Un équipement spécifique et coûteux est donc nécessaire pour l'atteindre, ce qui explique que les acteurs nationaux, seuls à détenir le matériel adéquat, aient conservé si longtemps le monopole des coupures de câbles en mer.

Les faits mènent désormais vers de nouvelles conclusions. En 2007, des pêcheurs vietnamiens ont coupé plus de 500 km de câble sous-marin afin d'y récupérer les matériaux composites et de tenter de les revendre. Le Vietnam perdra ainsi plus de 80 % de sa connectivité avec le reste du monde. Ce cas marque le début d'une série de sabotages effectués par des acteurs non étatiques sur les fils de fibre optique. Le constat est significatif : de simples pêcheurs sont désormais capables d'intervenir sur des câbles avec leur propre matériel, affectant le réseau pendant plusieurs semaines. Au Gabon, en mars et avril 2015, deux autres actes de vandalisme ont eu lieu. Une preuve supplémentaire que des actions privées sur le système sont envisageables. Enfin, la fameuse attaque du navire câblier en mer Rouge cet été est presque inédite dans le domaine de la piraterie maritime. Bien que repoussés par l'équipe de protection du navire, seize pirates armés auraient ainsi tiré sur le bâtiment alors en pleine opération de pose de fibre optique. Si ce type de navire est inscrit sur la liste des bateaux ciblés par la piraterie et vulnérables en raison de leur activité, les rapports annuels du Bureau maritime international (IMB) font remonter les derniers actes de ce type à 2003 et 2005.

Par ailleurs, l'action d'acteurs non étatiques sur la fibre optique pourrait être favorisée par la technologie. Le progrès des drones sous-marins (*unmanned autonomous vehicle*) en matière de pose et de maintenance semblent faciliter les opérations sur les câbles sous-marins, jusqu'alors longues et complexes. Permettant de manipuler les fils de fibre optique à distance dans des eaux profondes, ils se révèlent être l'avenir de la gestion du système sous-marin [Clark, 2016, p. 2]. Leur commercialisation croissante n'est cependant pas une nouvelle rassurante : des individus malintentionnés pourraient s'en procurer de manière plus aisée et agir sur les câbles.

Entre sabotage, piraterie et actions terroristes, la frontière n'est pas si évidente. Les inquiétudes américaines en la matière ne contribuent pas au relativisme. Si aucun acte terroriste sur les câbles n'a pour l'heure vu le jour, une série de coupures de câbles atterrissant en Californie a inquiété le Federal Bureau of Investigation (FBI) en 2015 [Lai Ki, 2016, p. 52]. Soupçonnant une action coordonnée de nature terroriste, l'organisme américain a rapidement ouvert une enquête. La publication de documents officiels portant sur les vulnérabilités du réseau sous-marin par le



*Hérodote*, n° 163, La Découverte, 4e trimestre 2016.

département de la Sécurité intérieure du pays[9] appelle d'ailleurs à la vigilance. Motivations et conséquences d'une action terroriste sur les sites d'atterrissement américains y apparaissent : manque de diversité des stations d'atterrissement sur le territoire des États-Unis, concentration importante des câbles sous-marins, facilité d'action, rentabilité et rayon d'action d'une attaque sur l'infrastructure de télécommunications... Les arguments ne manquent pas [Lacroix *et al*., 2002, p. 142].

Cette éventualité reste cependant au stade de prospective, l'actualité nous rappelant la pérennité de l'intérêt national porté à ces infrastructures. L'inquiétude du gouvernement américain au sujet du navire océanographique russe *Yantar*, l'an passé, l'a illustré. Naviguant à proximité des câbles reliant les États-Unis au reste du monde, plusieurs autorités se sont exprimées sur le sujet, traduisant une préoccupation étatique importante. De même, le piratage du site d'administration et de gestion du câble sous-marin SEA-ME-WE 4, reliant la France à Singapour, par la National Security Agency (NSA) montre la capacité d'action encore détenue par les États sur cette infrastructure[10]. En termes d'espionnage, les révélations sur les programmes *Tempora* ou *Upstream* de la NSA par Edward Snowden en 2013 reflètent, elles aussi, l'intérêt durable que porte l'acteur national au système sous-marin de télécommunications.

## Sécuriser le réseau sous-marin mondial

La reconnaissance de l'attaque en mer Rouge comme un acte de piraterie, non encore officielle, pourrait marquer un tournant dans le domaine de la protection des câbles sous-marins. Depuis 1869, des propositions sont émises pour mieux protéger l'infrastructure sous-marine des dégradations volontaires [Voelckel, 2012, p. 272]. La théorie consiste à les assimiler à des actes de piraterie, afin de combler le manque de protection juridique et de faire face aux cas complexes. Les Nations unies favorisent, il est vrai, la coopération entre États ainsi que la répression et le contrôle des actes de piraterie, alors que rien n'est spécifiquement prévu à ce jour pour lutter contre les dégradations volontaires du réseau sous-marin. Il n'existe d'ailleurs pas, à ce jour, de statut légal du pillage des câbles en haute mer. Seules des mesures punitives sont prévues : tous les États parties à la convention des Nations unies sur le droit de la mer doivent ériger en infractions les atteintes volontaires ou par négligence aux câbles sous-marins en haute mer, dans la mesure où un risque de perturbation ou

9. DHS, Protective Security Division, *Potential indicators of terrorist activity infrastructure category* : *cable landing stations*, 30 janvier 2004.

10. « La NSA a piraté un réseau Internet français pour accéder aux données d'un câble sous-marin », <www.lemonde.fr>, 30-12-2013.

d'interruption des communications s'ensuivrait [Voelckel, 2012, p. 272]. Associer le pillage ou la coupure des câbles sous-marins à des actes de piraterie pourrait en garantir une meilleure protection [Burnett et Green, 2008, p. 581]. Cette possibilité permettrait en effet de réagir plus rapidement en étendant le régime existant à ce nouveau défi, au lieu de construire une nouvelle structure juridique spécifique. Cependant, la notion de piraterie ne connaît pas, en droit international, d'interprétation uniforme. Pour une partie de la doctrine, les motifs des pirates doivent être nécessairement privés. Si la plupart des sabotages référencés ici entreraient donc bien dans le cadre décrit, les actes terroristes sur les câbles, aux fins « politiques », en seraient exclus [Burnett et Green, 2008, p. 574]. Par ailleurs, deux bateaux devant être impliqués dans les faits pour pouvoir faire référence, au sens strict, à des actes de « piraterie », nombre des cas cités ne pourraient recevoir une telle qualification.

L'attaque du navire câblier à l'origine de notre réflexion ne semble donc pas remettre fondamentalement en question les vulnérabilités attribuées au réseau sous-marin, mais plutôt confirmer des tendances restées jusque-là discrètes – entrée en lice des acteurs non étatiques, croissance du nombre d'infrastructures câblières, de leur concentration, de leur importance pour l'économie mondiale et de leur visibilité, le tout cumulé à un progrès technologique rapide dans le domaine... – et pour lesquelles la sécurisation des câbles est insuffisante. Des initiatives nationales comme internationales émergent aujourd'hui afin d'assurer la protection du système câblier dans son ensemble. Elles consistent en l'amélioration de la communication et de la fluidité de l'action. Des propositions d'harmonisation internationale et d'intervention en coopération sont notamment formulées. Elles concernent par exemple le développement de point de contact unique par pays servant de relais pour les compagnies de télécommunications, d'accords et d'entraînements communs entre les forces navales ou encore de facilitations des procédures d'autorisation pour les sorties en mer, afin d'agir face à de tels actes [Burnett et Green, 2008, p. 582]. Au niveau national, seuls les États-Unis ont réellement pris la mesure de cette exigence : la Federal Communications Commission[11] (FCC) a notamment mis en place cette année un système de report des dommages sur les câbles sous-marins desservant le pays. L'objectif est ainsi d'améliorer le processus de réponse face à une interruption de service afin de restaurer au plus vite le réseau et d'assurer la permanence des télécommunications. L'idéal serait à présent que les autres pays suivent cet élan et que des mesures soient prises au niveau global, avant qu'un fait plus grave n'intervienne sur le réseau sous-marin mondial...

11. La Federal Communications Commission est une agence indépendante du gouvernement des États-Unis. Créée par le Congrès américain en 1934, elle est notamment responsable de la régulation des télécommunications et d'Internet.

## Bibliographie


BURNETT D.R. et GREEN M.P. (2008), « Security of international submarine cable infrastructure : time to rethink ? », *Legal Challenges in Maritime Security*, Leyde, p. 557-583.

CLARK B. (2016), « Undersea cables and the future of submarine competition », *Bulletin of Atomic Scientists*, vol. 72, n° 4, p. 234-237.

DHS, DEPARTMENT OF HOMELAND SECURITY (2004), Protective Security Division, *Characteristics and Common Vulnerabilities Infrastructure Category : Cable Landing Stations*.

GALLAND J.-P. (2010), « Critique de la notion d'infrastructure critique », *Flux*, n° 81.

JACOB P. (2000), *Internet, nouvel espace maritime ? Éléments d'une géopolitique d'internet*, Collège interarmées de défense (CICDE).

JOHNSON C.W. (2013), « The Telecoms inclusion principle : the missing link between critical infrastructure protection and critical information infrastructure protection », *in* Paul THERON et Sandro BOLOGNA (dir.), *Critical Information Infrastructure Protection and Resilience in the ICT Sector,* IGI Global, p. 277-303.

LACROIX F., BUTTON R., JOHNSON S. et WISE J. (2002), *A Concept of Operations for a New Deep-Diving Submarines*, Santa Monica, Rand Corporation.

LAI KI C. (2016), « Optical collusion, undersea data cables at risk of interception », *IHS Jane's Intelligence Review*, p. 50-53.

MATIS M. (2012), *The Protection of Undersea Cable, a Global Security Threat*, United States War College, Strategy research project.

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.

SALVADOR R., FOUCHARD G., ROLLAND Y. et LECLERC A.P. (2006), *Du morse à l'Internet : 150 ans de télécommunications par câbles sous-marins*, La Seyne-sur-Mer, AACSM.

SECHRIST M. (2010), « Cyberspace in deep waters : protecting the arteries of the Internet », *Harvard Kennedy School Review*, vol. 10.

SIBONI G. et MAGEN Z. (2016), *The Cyber-Attack on The Ukrainian Electrical Infrastructure : Another Warning,* INSS Insight, n° 798.

VOELCKEL M. (2012), « Des mots sous la mer : à propos de la convention de Paris du 14 mars 1884 pour la protection des câbles sous-marins », *Annuaire du droit de la mer*, Paris, Pedone.