Observatoire du Monde Cybernétique
Trimestriel

Décembre 2013

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Sommaire

1. Cyberdjihad : l'apport d'Internet au djihad

« C'est l'Internet qu'Allah emploie au service du jihad et des moudjahidines, car la moitié de la bataille est menée sur les sites Internet »

Le cyber djihad est l'utilisation d'Internet pour l'accomplissement des objectifs stratégiques et tactiques de la guerre sainte islamiste. L'organisation djihadiste phare, Al-Qaïda, a d'une certaine façon réussi à combiner une idéologie née au 14ème siècle et l'utilisation des technologies[1] du 21ème siècle afin d'attirer des adeptes et attaquer ses ennemis. Les récentes actions extrémistes (réussies ou non) se sont basées sur un usage extensif d'Internet pour recruter, communiquer et coordonner une attaque, comme ce fut le cas pour l'attentat du marathon de Boston, la fusillade de Fort Hood et les attentats à la bombe de Londres en 2005. Le cyber djihad est en parfaite adéquation avec la stratégie d'Al-Qaïda qui se base sur des cellules dispersées et indépendantes, pouvant mener par elles-mêmes des actions ou rejoindre des groupes plus larges (par exemple dans des camps d'entraînement). En réponse au cyber djihad, des organisations antiterroristes internationales ont créé des réseaux facilitant les échanges d'informations permettant de repérer, disperser et arrêter des cellules terroristes. Ce type de coopération a porté ses fruits bien que le combat contre le cyber djihad soit loin d'être aisé pour ces organisations.

« Djihad » est un terme arabe signifiant « lutter », ou « exercer une force ». C'est un concept qui dispose de nombreuses acceptions. Si l'une des formes du djihad reste le djihad spirituel, par le cœur, l'acception du djihad dit « par l'épée » reste fortement répandue. Popularisée par l'usage qu'en font les groupes terroristes islamistes extrémistes, c'est en ce sens que le terme « djihad » est ici utilisé.

Le cyber djihad diffère principalement du cyber terrorisme en ce qu'il consiste en la diffusion de l'information au nom d'une organisation ou d'un djihadiste isolé, alors que le cyber terrorisme désigne les attaques de hackers dans le cadre d'une guerre économique, politique et psychologique. Le cyber djihad mène la guerre sainte au nom d'Allah dans un espace nouveau et immédiat ; les leaders des organisations terroristes, dont Oussama Ben Laden, ont ainsi mis en avant le fait que les médias djihadistes étaient, au même titre que le djihad, au cœur du champ de bataille[2]. Un individu sur le forum al-Hesbah a résumé le cyberdjihad comme suit « C'est l'Internet qu'Allah emploie au service du jihad et des moudjahidines, car la moitié de la bataille est menée sur les sites Internet ».

[1] http://www.foreignpolicy.com/articles/2013/04/29/how_to_defeat_cyber_jihad#sthash.DZxKsYnw.dpbs
[2] Gregory S. McNeal. "Cyber Embargo: Countering the Internet Jihad" Case Western Reserve University Journal of International Law 39 (2008)

Le leader actuel d'Al-Qaïda, Ayman Al-Zawahari, a également indiqué dans une lettre : « nous sommes dans la bataille des médias, pour les esprits et les cœurs de notre Umma »[3].

Les djihadistes se servent de l'anonymat et de l'absence de frontières sur Internet pour faire avancer leur cause. Internet est utilisé à chaque étape du processus de radicalisation, et ce jusqu'à la réalisation de l'attaque physique.

Les quatre étapes de ce processus sont : la pré-radicalisation, l'auto-identification, l'endoctrinement et la djihadisation. Chacune de ces étapes utilise le web pour collecter des informations utiles à la cause du djihad, les partager et les protéger. Les "apprentis djihadistes", durant la première phase de pré-radicalisation, utilisent Internet pour satisfaire leur curiosité et se familiariser avec les fondamentaux. Typiquement, ils se lancent dans la lecture passive de forums pour en apprendre plus sur des sujets variés allant de la santé au militantisme, ou encore de l'histoire de l'islam aux technologies de l'information. L'auto-identification pousse ces personnes à contribuer de plus en plus activement aux discussions relatives au djihad sur les forums et échanger avec d'autres partageant les mêmes idéaux. La phase d'endoctrinement se caractérise par une activité en ligne plus agressive, telle que la prise de contact avec des guides spirituels radicaux, l'accès à des tutoriaux et des vidéos sur les aspects opérationnels du djihad - des manuels sur la mise en place d'une attaque. Enfin, la phase de djihadisation incorpore tous les comportements en ligne précédemment répertoriés, auxquels s'ajoutent des communications secrètes pour recruter des soldats, recueillir des informations et coordonner l'attaque souhaitée.

L'utilisation de cyberattaques par les djihadistes en tant qu'activité offensive en ligne est peu probable du fait du manque de ressources financières, techniques et de main-d'œuvre. Au mieux, des groupes de hackers djihadistes pourraient perturber l'accès à un site internet, mais n'ont pas les moyens de causer des dommages physiques par le biais de cyberattaques ciblées. A l'heure actuelle, le cyber djihadisme est essentiellement un moyen de diffusion et de mise en relation au service d'une cause, une ressource en soi. Ce faisant, il est devenu de plus en plus commun de voir des organisations terroristes s'appuyer sur Internet pour diffuser leurs propagandes et communiquer, plutôt que de mener des attaques. Internet a démontré être un des moyen les plus efficaces pour répandre une information à une audience partout dans le monde, avec des risques relativement faibles.

En fait, Internet est devenu le vecteur de communication stratégique et le djihad entend principalement attirer par ce biais les sympathisants, qu'ils soient musulmans de base ou convertis, et créer ainsi une **communauté virtuelle grandissante de djihadistes**. Internet, aisément accessible par des individus de chez eux ou dans des lieux publics, permet une croissance exponentielle des nouvelles recrues. Par conséquent, Internet est avant tout utilisé pour mettre en place un centre des

[3] http://www.dsalert.org/int-experts-opinion/homeland-security/515-cyber-jihad-osj-open-source-jihad
Umma - Muslim Community

opérations, recueillir des fonds, recruter des nouveaux djihadistes, les entraîner et les radicaliser, et motiver ceux souhaitant répandre l'idéologie. De manière plus indirecte, le djihad en ligne peut aussi être identifié comme une guerre psychologique qui maintient l'illusion d'une menace perpétuelle contre l'Ouest (qui est « le plus grand ennemi » - Kufar) à travers des publications régulières, des messages forts, la mise en ligne de vidéos d'otages et la description des attaques réalisées. Les publications djihadistes ont aussi pour but de légitimer la cause et diaboliser l'ennemi en insistant sur son caractère brutal et oppressif.

Moyens et fins de l'e-djihad

Les techniques utilisées pour diffuser la propagande, héberger les forums, lever des fonds, créer des manuels d'entraînement et des vidéos et mettre en place le réseau nécessaire à une opération sont très similaires à ceux utilisés normalement pour des activités en ligne - bien que la finalité diffère. Comme décrit auparavant, le cyber djihad est essentiellement une activité de collecte de ressources, qui ne requiert pas de matériel spécifique pour fonctionner efficacement. Cela dit, les ressources et les communications des djihadistes peuvent être cachées, tout particulièrement lorsque cela concerne l'entraînement et la planification d'opérations. La section qui suit entend suivre la chaîne de l'activité djihadiste en ligne, du début à la fin, du point de vue des djihadistes et du canal de distribution, en expliquant les méthodes techniques généralement employées dans le cadre du cyber jihad.

1.1 Top-Down : la dissémination de l'information

1.1.1 *Les sites Internet*

Les sites Internet djihadistes ne sont pas une nouvelle tendance, mais leur nombre a connu une forte croissance depuis la fin des années 1990 : ils sont passés de 28 en 1997 à plus de 5000 en 2005[4]. Les plus populaires sont ceux directement liés à Al-Qaïda (Al Fajr media centre, As Sahab, Global Islamic Front et Al Andalous).

Afin d'acheminer les informations de manière efficace, plusieurs canaux de diffusion sont mis en place. Il y a trois types de sites Internet djihadistes : les sites officiels, les blogs et les forums, et les sites des distributeurs. A travers des liens partagés, des livres et des références, ces sites créent une véritable toile d'informations djihadistes totalement décentralisée.

[4] Gabriel Weiman, Key note speach at OSCE Workshop on Combating the Use of the Internet for Terrorist Purposes, Vienna, October 2005

Les sites officiels sont gérés par des clercs dits "professionnels" ainsi que par des organisations dédiées. Ces sites ont pour but principal de diffuser largement la propagande à travers des textes religieux, des livres et des vidéos qui enseignent et incitent à la Guerre Sainte. Les dernières nouvelles, les communications interactives (via Skype), les lectures recommandées, les contacts et des questions/réponses peuvent être disponibles sur ces sites. Ces derniers sont typiquement disponibles sur l'Internet "ouvert", bien que beaucoup de liens postés sur ces sites aient une durée de vie très courte du fait des fermetures régulières. Les leaders religieux ou djihadistes tels qu'Oussama Ben Laden et Anwar Al Awlaki avaient leurs propres sites, extrêmement populaires du fait de leur célébrité. A partir de ceux-ci, des djihadistes peuvent parfois entrer en communication directe avec un leader si ce dernier accepte.

Les djihadistes "amateurs", plutôt que ceux ayant un vrai rôle opérationnel, sont généralement ceux qui hébergent les forums et les blogs. Le problème pour les djihadistes est que tout le monde peut avoir accès aux informations. Alors que toute personne intéressée peut se renseigner, les administrateurs des sites préfèreraient en réalité limiter le nombre de visiteurs et de contributions pour éviter que les sites ne soient saturés. Par conséquent, de nombreux forums et sites Internet imposent une procédure d'enregistrement, complétée par un nom d'utilisateur et un mot de passe. Régulièrement, toute personne souhaitant accéder au site devra démontrer son adhésion concrète au djihadisme à l'administrateur du site, qui a le pouvoir de supprimer les publications si celles-ci ne s'avèrent pas en faveur de la cause. Les sites mettent en place de plus en plus de filtres, certains sites nécessitant d'avoir reçu des invitations personnelles pour en obtenir l'accès : un possible obstacle pour les "loups solitaires", souvent éloignés de toute communauté musulmane majeure[5].

Ansar al haqq forum (A French Islamic Site)
Source: http://www.ansar-alhaqq.net/PDF/jihad.php

Les blogs sont également immensément populaires, et sont généralement vus comme à mi-chemin entre le site interactif et le site de distribution de contenu. La plupart des blogs présentent des liens

[5] http://privacy-pc.com/articles/jihadist-use-of-the-internet-2008-2011-overview-2-cyber-jihad-methods-and-tools.html

vers des sites Internet djihadistes, et permettent ainsi d'éviter des interférences telles que de fausses publications ou des spams[6]. De plus, ils peuvent permettre à de multiples auteurs de publier, et ainsi d'échanger des points de vue, des tactiques et des enseignements, le tout contrôlé par une autorité unique.

Enfin, il existe des sites de distribution. Ceux-ci cherchent à soutenir les infrastructures djihadistes en ligne en fournissant des liens dits « vérifiés » vers des sites djihadistes authentiques. Leur finalité est d'aider les nouvelles recrues, en leur offrant l'accès à un réseau et une très grande quantité de contenu fiable. La plupart des sites de distribution semblent construits sur des standards techniques plus élevés que les sites djihadistes classiques[7]. Un des sites de distribution le plus connu est le Global Islamic Media Front. Les organisations menant des opérations de propagande en association avec Al-Qaïda et d'autres groupes diffusent tant les contenus créés par des sites partenaires que leur propre contenu. Deux des contributions au djihad les plus importantes faites par le GIMF furent la diffusion du logiciel de chiffrement Moudjahidine Secrets, et le jeu vidéo Quest for Bush.

Quest for Bush Screenshot; Source: www.g4TV.com[8]

1.1.2 *Aspects techniques*

L'une des préoccupations principales des sites djihadistes est leur hébergement. Ces sites peuvent rester en ligne du simple fait que leur hébergeur n'est pas regardant sur la nature des sites qu'il héberge (hébergeur bulletproof). Lorsque les sites Internet incriminés sont fermés par les autorités, les djihadistes changent simplement d'hébergeur. Cette relocalisation, qui inclut également généralement le changement de nom de domaine[9], est une opération relativement lourde pour les groupes djihadistes qui perdent ainsi en influence et en affluence.

---

[6] http://www.fas.org/irp/world/netherlands/jihadis.pdf
[7] Hanna Rogan, JIHADISM ONLINE
[8] http://www.g4tv.com/thefeed/blog/post/711092/homefront-and-propaganda-in-video-games-what-are-they-trying-to-tell-you/
[9] A noter que le nom de domaine doit changer quand il est supprimé par un FAI, car le DNR peut retrouver le nouveau nom du FAI du nom de domaine dans son directoire et en informer les autorités.

Al-Qaïda a trouvé un moyen de contourner ces difficultés en utilisant des réseaux sécurisés. Lorsqu'un de leurs sites, ou tout autre site djihadiste, est fermé, Al-Qaïda utilise des "chats", des listes de mails et les sites de sympathisants pour informer du nouveau nom de domaine[10]. Si Al-Qaïda, l'organisation djihadiste phare, tire aisément profit de cette méthode, les groupes d'amateurs et les individus isolés doivent quant à eux repartir de zéro à chaque fermeture de site web. Dans ce cas, le seul moyen de suivre l'actualité des changements d'URL est de se référer aux forums et sites acceptant de rediffuser leur nouveau nom de domaine.

Les blogs et forums ont tendance à être plus flexibles et plus simples à mettre en place que les sites Internet statiques. Des outils de "blogging" gratuits et ouverts, tels que Wordpress, peuvent être utilisés par n'importe quel individu capable de télécharger la plate-forme. De manière similaire, les forums peuvent être créées simplement en achetant l'accès à un software open-source, tel que vBulletin, et ensuite hébergé et modéré selon les choix de l'administrateur. A titre d'exemple, le software vBulletin est possédé par une entreprise américaine et fait payer 180$ les achats de licence permettant de démarrer un forum.

1.1.3 *Social Media*

L'utilisation des médias sociaux par les djihadistes à des fins de propagande constitue une tendance lourde. Facebook, Twitter ou encore YouTube servent à des fins de propagande ciblant un public le plus large possible.

Régulièrement, les djihadistes postent des vidéos d'attaques contre des troupes occidentales et leurs alliés. Et bien que celles-ci soient supprimées très rapidement, elles sont rapidement partagées avant leur suppression, afin d'être sauvegardées et republiées sur d'autres médias sociaux. L'objectif de certaines vidéos est de susciter l'imitation de masse. Par exemple, la vidéo d'un extrémiste islamiste attaquant des avant-postes américains en Afghanistan à l'aide d'une moto a été largement diffusée. A la suite de sa publication sur YouTube, un grand nombre d'attaques similaires a eu lieu dans le pays. Cette d'attaque n'était pas seulement intéressante par son efficacité, mais également par son aspect attractif pour les jeunes qui trouvaient le mode opératoire spectaculaire tentaient de le reproduire.

[10] Gregory S. McNeal. "Cyber Embargo: Countering the Internet Jihad" Case Western Reserve University Journal of International Law 39 (2008)

De même, de nombreuses vidéos sur YouTube appellent au jihad en Syrie en pariant sur le sentiment d'indignation face à la violence que les visiteurs des sites ressentent en regardant les vidéos. Un djihadiste français indique dans une vidéo qu'il "y a beaucoup de Musulmans dans le monde, et qu'ils [les rebelles syriens] ont besoin d'eux", tout en portant une Kalachnikov, un foulard et le drapeau blanc et noir d'Al-Qaïda derrière lui[11].

Two French jihadists in Syria ; Source : BBC News[12]

[11] http://www.reuters.com/article/2013/09/04/us-syria-crisis-internet-insight-idUSBRE9830OW20130904
[12] http://www.bbc.co.uk/news/world-europe-23766892

Source : http://atlasshrugs2000.typepad.com/atlas_shrugs/cyber_jihad/

1.2 Bottom-Up : monter dans la hiérarchie djihadiste

1.2.1 *Radicalisation et entraînement*

Entre les premières manifestations d'intérêt pour le mouvement djihadiste et l'entrainement intensif, l'apprenti-djihadiste passe la majorité de son temps à s'éduquer, lire et à échanger en ligne. Cette période dure en moyenne deux ans. Le djihadiste en devenir se renseignera sur la cryptographie, sur TOR, et d'autres méthodes permettant de sécuriser les données et leur transmission. L'Internet, en tant que moyen permettant d'accéder rapidement à l'information, est ici un avantage majeur ainsi qu'un support clé pour l'approfondissement et l'élargissement du mouvement djihadiste. Un simple blog ou forum peut ouvrir les portes d'un large éventail d'autres sites ou forums djihadistes. A partir de ces ressources disponibles, le djihadiste aura accès à de nombreux axes de réflexion et, au fur et à mesure de la lecture, affinera ses centres d'intérêt. Les sujets abordés peuvent aller de la science à l'Histoire, mais avec pour thème constant l'islam fondamentaliste et le Salafisme. De nombreuses discussions tournent en effet autour des textes religieux appliqués aux derniers évènements vécus par des individus ou par la communauté musulmane toute entière. Malgré le fait que la majorité des interprétations des textes soient grossièrement sortie de son contexte pour correspondre à la vision et l'idéologie des rédacteurs, les jeunes musulmans lisant les discussions semblent y adhérer aisément. L'information est généralement disponible en arabe, et de plus en plus en anglais. Des traductions en français, allemand, néerlandais sont également parfois réalisées. Ces traductions ont pour but d'attirer un maximum de musulmans et de convertis potentiels vivant à l'Ouest, et susceptibles de se joindre à

l'"Umma" dans son combat contre les incroyants. Cela alimente un sentiment d'appartenance pour les "loups isolés" vivant dans ces pays[13].

Après cette phase d'apprentissage par la lecture, l'apprenti-djihadiste diffusera à son tour du contenu à caractère "éducatif". L'aspect technique de cette seconde phase est, une fois encore, assez classique tant que le contenu publié est diffusé sur l'Internet "ouvert". Le point négatif de ces sites pour les djihadistes continue d'être l'accès ouvert à l'information. Les administrateurs aimeraient en effet pouvoir savoir qui visite et contribue aux sites djihadistes. Par conséquent, de nombreux forums et sites Internet requièrent l'enregistrement de tout utilisateur. Occasionnellement, la personne demandant un accès au site devra prouver sa sympathie pour la cause djihadiste.

Un djihadiste motivé à la recherche d'entraînements se tourne vers les vidéos et les manuels disponibles sur de très nombreux sites, allant de YouTube aux sites d'Al-Qaïda. Alors que la plupart des vidéos publiées sont faites pour choquer l'ennemi et inspirer les alliés, d'autres sont mises en ligne dans le but de former les intéressés. Ces entraînements vidéo peuvent par exemple porter sur les tactiques de guérilla ou l'utilisation d'armes à feu. Les entraînements dispensés par manuel reprennent des procédés techniques assez poussés tels que la confection de bombes artisanales ou la fabrication de poison. Il existe de nombreux livres et articles sur ce type d'informations, la plupart venant d'auteurs occidentaux (anarchistes par exemple). Aussi, des tutoriaux sur le renseignement ouvert, le chiffrement ou le code informatique sont diffusés entre djihadistes afin d'améliorer le niveau de connaissances technologiques dans leurs rangs.

Parmi les phénomènes islamiques les plus pertinents, il faut noter l'existence de l'Université d'Al-Qaïda pour les sciences du Jihad. La première personne à utiliser cette appellation soutenait ainsi qu'Al-Qaïda était à la fois une organisation, un Etat et une université. L'essence de cette trinité se base sur les trois corps formant ainsi un seul élément. Une idéologie issue d'une école de pensée représentant la volonté de certains d'apprendre et d'appliquer les méthodes du djihad. Cette "université" est entièrement numérique, décentralisée et sans frontières. Ses diplômés sont spécialisés dans le cyber, les médias, le financement du djihad en plus des connaissances essentielles en morale et, de façon plus originale, en explosion de voiture[14].

1.2.2 *Recrutement*

Une des caractéristiques des recrues pour le djihad est leur jeune âge. Anwar al-Awlaki[15] voulait en effet s'assurer que les enfants reçoivent une éducation Salafiste le plus tôt possible, afin qu'ils soient endoctrinés et formatés à la manière des cyber moudjahidines. L'objectif étant de remplacer leurs

[13] http://www.fas.org/irp/world/netherlands/jihadis.pdf
[14] http://www.freerepublic.com/focus/f-news/1505115/posts
[15] Un des recruteurs d'arabophones et d'anglophones les plus importants.

activités en ligne par des actions physiques contre des cibles dites "soft" ou "hard"[16]. Le cyberdjihad s'est ainsi adapté à la jeunesse des recrues par la création de jeux vidéo thématiques afin de contribuer au développement de pensées extrémistes au sein des populations musulmanes dès l'enfance.

Le recrutement des djihadistes est un processus protéiforme qui dure de plusieurs mois à plusieurs années. Il peut prendre deux formes principales : l'une passive et involontaire, l'autre plus directe, plus agressive. La première forme peut consister en de la propagande (multimédia, jeux vidéo, livres, etc.) et des enseignements collectifs en ligne intégrés en parcourant des sites et des forums djihadistes. Ce recrutement vise large, et cherche à attirer un maximum de personnes. Par cette méthode, de nombreux individus intéressés par les mouvements djihadistes vont "s'auto-recruter" et agir seuls ou en petits groupes. Cette première méthode n'exclut pas que des leaders recrutent eux-mêmes directement ou choisissent de guider des individus à distance.

Les individus motivés et proactifs cherchent tôt ou tard à entrer en contact avec un leader religieux. Une fois ce dernier informé des intérêts et des aspirations du candidat, il utilise ces éléments pour intégrer l'individu dans un schéma de recrutement motivant, tout en l'accompagnant dans un processus qui se conclut par la planification et l'exécution d'une attaque physique. Un des recruteurs d'arabophones et d'anglophones les plus importants fut Anwar Al-Awlaki. Il fut impliqué dans de nombreuses vidéos d'entraînement, de motivation, réalisa des cours en ligne et participa à de nombreux échanges en ligne avec ses partisans afin de faire progresser le djihad.

Al-Awlaki aurait été associé à la planification de l'attentat à la bombe de 2009 sur un avion en direction de Detroit, baptisé "Christmas Day Bombing". Le terroriste nigérian Umar Farouk Abdulmutallab responsable de l'attaque aurait été dirigé vers un camp d'entraînement au Yémen par Al-Awlaki, après avoir été recruté par ce dernier suite à un cours en ligne. Lors de son arrestation, Abdulmutallab aurait indiqué avoir été personnellement entraîné lors de son séjour dans le camp par Al Awlaki, tandis que des renseignements montraient que les deux protagonistes s'étaient effectivement rencontrés pour préparer l'opération. L'attaque ratée qui eut finalement lieu se déroula lors d'un vol entre Amsterdam et Detroit, à l'aide d'explosifs cachés dans les sous-vêtements d'Abdulmutallab.

Al-Awlaki serait également associé, entre autres, aux attentats du 11 septembre 2001, de Londres en 2005 et de Fort Dix en 2007. Toutes ces opérations avaient pour dénominateur commun les enseignements d'Al-Awlaki, qui auraient grandement influencé les terroristes sans que des communications directes aient pour autant été établies.

[16] http://privacy-pc.com/articles/jihadist-use-of-the-internet-2008-2011-overview-2-cyber-jihad-methods-and-tools.html

Source : http://pibillwarner.wordpress.com/ 17

Selon une personne haut placée au Department of Homeland Security américain, le recrutement des djihadistes a augmenté exponentiellement en ligne du fait de deux facteurs[18]. Le premier est l'utilisation de Facebook, de YouTube, et la sophistication croissante dans l'usage d'Internet. Le second facteur est le fait que les centres de recrutement "classiques" (les mosquées et les centres communautaires), sont de plus en plus surveillés, ce qui pousse les individus à mener leurs actions en ligne où la surveillance est bien plus faible. Le recrutement en ligne a cependant ses limites : il est moins direct que des rencontres organisées en personne et requiert un certain degré d'anonymat[19].

Les djihadistes peuvent être mis en contact avec des camps d'entraînement de terroristes, qui organisent le voyage permettant aux nouveaux candidats de les rejoindre. Une fois que le djihadiste passe avec succès l'épreuve de l'enquête de sécurité (pouvant prendre entre neuf et douze mois), il peut enfin être entraîné pour mener des opérations au Moyen-Orient, des attaques dans un pays occidental, ou renvoyé dans son pays d'origine afin qu'il aide à son tour au recrutement.

1.2.3 *Chiffrement et protection*

Afin de conserver leurs communications privées, les djihadistes utilisent des "drop box", des méthodes de sténographie et de chiffrement. Alors que le chiffrement est devenue monnaie courante, la sténographie serait rapidement tombée en désuétude. Les "drop box" sont ici l'un des moyens les plus utilisés. Il s'agit de placer des informations dans un e-mail sauvegardé en tant que "brouillon" plutôt qu'envoyé. L'utilisateur peut alors se déconnecter, donner les identifiants à un tiers qui pourra accéder aux brouillons enregistrés sur la boîte mail. La sténographie est une

[17] http://pibillwarner.wordpress.com/2011/10/03/terror-cleric-anwar-al-awlaki-lives-on-with-the-internet-shut-down-al-qaeda-linked-websites-and-videos-says-private-investigator-bill-warner/
[18] http://www.nytimes.com/2009/12/16/opinion/16friedman.html
[19] Hanna Rogan, JIHADISM ONLINE

méthode qui consiste à intégrer des messages dans des documents graphiques[20]. Il est difficile de savoir dans quelle mesure cette méthode est utilisée car elle est très difficile à détecter.

Le chiffrement, comme mentionné auparavant, peut être enseigné aux djihadistes par le biais de rapports et de manuels disponibles en ligne. Quand de jeunes djihadistes cherchent l'éclairage de chefs religieux ou djihadistes, ils doivent passer par des messages chiffrés, anticipant ainsi le cas où le "guide" leur indiquerait d'organiser une attaque. L'ex-leader d'Al-Qaïda, Anwar Al-Awlaki, a fréquemment pressé pour la création par les djihadistes de deux programmes de chiffrement qui ne seraient utilisés que par ces derniers : Moudjahidine Secrets and Tadpole.

Moudjahidine Secrets est un programme qui garantit un haut niveau de chiffrement protégeant les communications privées. Les éléments clés de ce programme sont le chiffrement symétrique, des clés publiques, la destruction régulière des données ainsi qu'une messagerie sécurisée[21]. Ce logiciel est encore utilisé aujourd'hui comme un standard pour les communications des djihadistes et a même été adapté pour les téléphones BlackBerry.

Page d'accueil de Mujaheddeen Secrets 2[22]

Tadpole a quant à lui été créé par Jamaat-ul-Mujahideen Bangladesh, une organisation islamiste de résistance. Le logiciel a été pour la première fois présenté par un jeune djihadiste bengali, Rajib Karim, à Anwar Al-Awlaki. Alors que ce dernier avait conseillé Rajib Karim d'utiliser Moudjahidine

[20] Timothy L. Thomas, Al Qaeda and the Internet: The Danger of "Cyberplanning, " 33 PARAMETERS, Spring 2003 at 112, available at http://www.carlisle.anny.mil/usawc/ Parameters/03spring/thomas.pdf
[21] http://ddanchev.blogspot.fr/2008/01/mujahideen-secrets-2-encryption-tool.html
[22] http://security-labs.org/fred/docs/08-rdn-crypto/

Secrets, le jeune ingénieur en informatique avait insisté pour utiliser Tadpole. Al-Awlaki adopta finalement le nouveau logiciel. L'hésitation de Rajib Karim à utiliser Moudjahidine Secrets était liée au fait qu'il est possible de le télécharger sur des forums ouverts, et que des experts en informatique occidentaux pouvaient donc l'avoir en leur possession et chercher à en casser le chiffrement. Malgré l'expertise de l'ingénieur bengali, le système de chiffrement de Tadpole qui fut aisément cassé a mené à son arrestation[23].

Le chiffrement n'a pas toujours été une constante dans la manière dont les djihadistes recrutent, communiquent et s'organisent. La préparation du 11 septembre 2001 s'est par exemple faite par le biais de services mails classiques et de codes au sein des messages, sans utiliser de logiciel de chiffrement.

The Onion Router (TOR) est également un moyen de chiffrement utilisé par les djihadistes. En installant le logiciel librement disponible sur Internet, les djihadistes peuvent avoir accès "Deep Web" et ainsi renforcer leur anonymat. Le "Deep Web" facilite entre autres l'achat d'armes et de composants permettant la mise en place d'une attaque (explosifs, ingrédients, etc.).

Les djihadistes sont également très préoccupés par la sécurité de l'information, non seulement pour protéger leurs données contre les gouvernements et les "veilleurs" (watchdogs), mais également pour se protéger des virus affectant tous les ordinateurs sans distinctions. Ils utilisent de nombreux anti-virus, dont Kaspersky. Pour les antivirus, ils se communiquent la clé ainsi qu'un guide sur l'installation du programme[24].

1.2.4 *Le loup isolé*

Les médias sociaux ont prouvé qu'ils sont essentiels au loup isolé, car ils lui donnent le courage de s'investir dans le djihad. Comme il a été décrit plus haut, les apprentis peuvent être recrutés simplement sur la base d'informations postées sur les sites djihadistes. Ces personnes sont appelées "self-igniters" (auto-enflammées), car elles n'ont pas besoin d'établir des communications avec d'autres djihadistes pour s'engager. Une fois ce stade atteint, le djihadiste peut soit se lancer seul dans une attaque, soit tenter de rejoindre un cercle de djihadistes en se servant des contacts disponibles.

Un exemple connu est celui de "Jihad Jane" qui a récemment été condamnée à 10 ans de prison. Jihad Jane est une femme américaine convertie à l'islam en 2007[25] à l'âge de 45 ans. Suite à sa conversion, elle s'est radicalisée en visionnant des vidéos de violences infligées par les américains et

[23] http://privacy-pc.com/articles/how-terrorists-encrypt-7-peculiarities-of-encryption-using-tadpole.html
[24] http://privacy-pc.com/articles/jihadist-use-of-the-internet-2008-2011-overview-2-cyber-jihad-methods-and-tools.html
[25] L'intérêt de Jihad Jane pour l'islam est né d'une romance qu'elle a eu avec un musulman. Sa vie perturbée (pédophilie, prostitution, consommation de drogue) a contribuée a son changement de vie.

les israéliens à des enfants palestiniens. Elle s'est par la suite fréquemment manifestée sur les forums et sites Internet djihadistes. En 2008, elle a gagné le respect d'organisations terroristes du fait de sa ténacité et de sa capacité à recruter de nouveaux combattants. Sur ordre d'un agent d'Al-Qaïda, elle tenta en 2009 d'assassiner un artiste suédois. Elle fut rapatriée aux Etats-Unis et arrêtée après l'échec de sa tentative[26].

En tant qu'éléments atypiques des organisations terroristes, les loups isolés se sentent souvent entourés par leurs ennemis proclamés. Cette situation peut générer chez eux des sentiments de colère ou de profonde dépression et favoriser leur radicalisation. De ce fait, la moindre communication avec un autre djihadiste peut considérablement renforcer leur sentiment d'appartenance au djihad et les motiver à entreprendre des attaques physiques. Comme l'a déclaré Jihad Jane "J'aimais tellement mes frères : lorsqu'ils me disaient quelque chose, je les écoutais quoi qu'il arrive. Et j'étais également… perdue."

1.2.5 *Capacités cyber*

Une cyberattaque majeure venant d'une organisation djihadiste est aujourd'hui peu probable. Les djihadistes formés à l'informatique peuvent mener des attaques par Déni de Service Distribué (DDoS) ou lancer différents virus, mais rien qui ne puisse causer des dégâts physiques. Les méthodes utilisées sont généralement les mêmes que celles employées par les fraudeurs et les hacktivistes. Ils peuvent donc altérer le trafic Internet et potentiellement hacker les profils sur des médias sociaux, mais manquent de ressources qui permettraient de conduire des opérations de cyber espionnage ailleurs que sur l'Internet "ouvert". Le cyber djihad utilise principalement Internet à des fins de commandement et de contrôle. La fraude en ligne peut cependant être une pratique courante afin de financer le djihad.

Les opérations de hacking ou les cyber attaques majeures sont pour l'instant attribuées à des Etats et – de manière croissante – à des acteurs soutenus par des Etats. Cependant, les Etats qui choisissent de fermer les yeux sur les mouvements djihadistes ou de les soutenir indirectement ne semblent pas disposer des capacités nécessaires pour contribuer à l'élaboration d'une cyberattaque majeure. Il reste cependant la possibilité de mener une attaque physique contre une infrastructure critique occidentale qui causerait une coupure d'Internet. Ce type d'attaque reste peu intéressant en raison de l'impact modéré qu'il aurait pour la cause : Internet serait restauré rapidement, l'impact psychologique sur les populations ne serait pas aussi significatif que dans le cas d'une attaque menée contre une cible plus traditionnelle. Une attaque suicide est ainsi considérée comme plus en raison de sa portée psychologique forte, mais aussi parce qu'elle permet la valorisation du martyr au sein des organisations djihadistes.

[26] http://www.reuters.com/article/2014/01/01/us-usa-terrorism-idUSBREA000HT20140101

1.3 Combattre le Cyber Djihad

Il est illusoire d'imaginer endiguer le cyber djihad grâce aux moyens coercitifs classiques. Internet est trop étendu, poreux et décentralisé. Si certains pays occidentaux tels que les Etats-Unis peuvent se servir de leviers juridiques, économiques, ou jouer sur la réputation des entreprises pour obtenir la fermeture de sites, cela ne perturbe pas les groupes djihadistes qui vont simplement changer de prestataire jusqu'à en trouver un qui ferme les yeux ou soit sympathisant de leur cause. Ce "jeu du chat et de la souris" est alors récurent.

"Watchdogs" et contre-espionnage

Face à la difficulté pour les gouvernements et les entreprises de patrouiller sur les vastes réseaux Internet, des sites de "Watchdogs" ont émergé dans le but d'apporter leur soutien dans la localisation

et la fermeture de sites Internet djihadistes. Un des plus connus est Internet Haganah. Ce site est animé par une petite équipe d'experts en terrorisme et de chercheurs sur Internet qui, malgré leur amateurisme, ont été capables de trouver des sites Internet djihadistes et d'attaquer la réputation des fournisseurs d'accès à Internet afin de les contraindre à fermer le site[27]. Les tactiques d'Internet Haganah ont été copiées par des agences de renseignement.

Le contre-espionnage est également privilégié. Les sites djihadistes sont intentionnellement laissés en activité par les services de renseignement afin de permettre leur infiltration, mais surtout de mieux comprendre leurs modes opératoires.

Alors qu'Internet Haganah se focalise sur le démantèlement des sites Internet djihadistes, deux autres groupes de "watchdogs" cherchent à produire du renseignement brut sur les dernières actualités des djihadistes ainsi que sur leur activité en ligne. SITE (Search for International Terrorist Entities) et Intelcenter, deux "watchdogs" basés aux Etats-Unis, sont passés de petits groupes d'amateurs au statut d'acteur majeur de la lutte contre le cyber djihad. Les deux entreprises se sont par exemple révélées capables de pénétrer les réseaux djihadistes bien plus en profondeur que plusieurs agences de renseignement. Ils sont en effet capables de traduire et transmettre rapidement des informations précises, parfois même avant leur découverte par les services gouvernementaux, et peuvent apporter des rapports d'analyse sur des évènements ou des tendances en ligne[28].

[27] http://gsmcneal.com/wp-content/uploads/2010/09/McNealJihadistWebsitesTestimony.pdf
[28] http://www.spiegel.de/international/world/insights-into-the-cyber-jihad-tracking-the-terrorists-online-a-575276.html

Au-delà des tactiques anti-djihadistes en ligne, les Etats-Unis ont formulé une stratégie qui consiste à faire circuler en ligne une vision plus modérée de l'islam ainsi que des vidéos montrant les atrocités effectuées par des extrémistes islamistes. Ces opérations psychologiques se sont révélées inefficaces car, d'une part, l'immense majorité des musulmans sont modérés et rejettent l'extrémisme et, d'autre part, les djihadistes ont rapidement mis en place des opérations pour contrer la propagande américaine, notamment en diffusant des photos et des vidéos d'abus d'exactions de soldats américains tels qu'à Abu Grahib[29].

1.4 Conclusion

Internet est généralement utilisé comme structure de soutien au djihad classique. Le renforcement considérable du djihad, tout particulièrement depuis les attaques du 11 septembre, et le développement en parallèle d'Internet a permis l'émergence d'une base de données essentielle à tout apprenti djihadiste. Même si ces derniers sont loin derrière leurs ennemis occidentaux en termes de moyens et de savoir-faire technologique, les djihadistes restent compétents et capables de développer les outils adaptés aux besoins des organisations en termes de discrétion et d'anonymat. Ils ont su tirer parti du succès des médias sociaux, comprenant que 90% du djihad repose sur une guerre de l'information. Leur propagande est efficace du fait de la récurrence de certains thèmes et des efforts de recrutement soutenus.

Plus de 600 musulmans européens se sont rendus en Syrie pour combattre le régime de Bachar al-Assad dans les rangs du djihad, la plupart influencés par les actualités postées sur les sites et les réseaux sociaux djihadistes. Ce phénomène est inquiétant pour deux raisons : le retour de ces djihadistes en Europe et l'impuissance des autorités face à la diffusion des informations favorables à la cause du djihad sur Internet.

[29] http://www.foreignpolicy.com/articles/2013/04/29/how_to_defeat_cyber_jihad

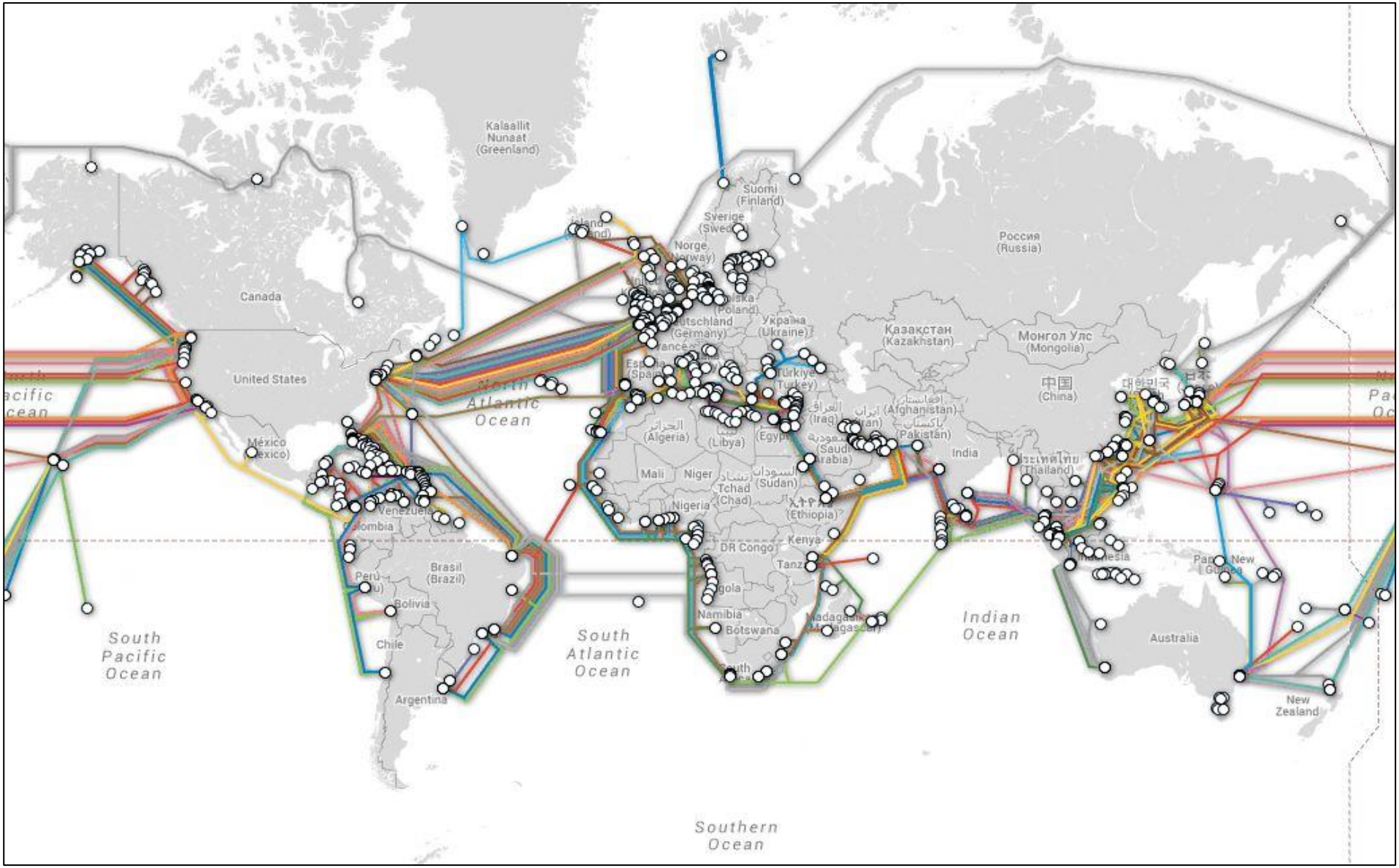
2. L'utilisation stratégique des câbles

Les 265 câbles aujourd'hui en service transportent 99% des échanges intercontinentaux de données. Leur dimension internationale n'est pas synonyme de neutralité: si la rentabilité économique et les contraintes géographiques semblent déterminer le tracé des câbles, des enjeux stratégiques sous-jacents sont aujourd'hui de plus en plus visibles.

Au-delà des enjeux économiques qui leur sont liés, les câbles peuvent également être de précieuses sources de renseignement, grâce à l'installation de dispositifs de collecte de données "upstream". Les révélations d'Edward Snowden ont récemment accéléré la prise de conscience d'un réseau de câbles trop centré sur l'Amérique du Nord et l'Europe, et des avantages stratégiques dont pouvaient bénéficier les pays se trouvant sur le trajet des câbles. Largement publicisées, les méthodes de collecte de données à même les câbles de la National Security Agency (NSA) américaine - en coopération avec d'autres Etats ou de manière clandestine - ont suscité la formulation de stratégies alternatives, en réaction à la position aujourd'hui dominante de Washington.

La volonté d'éviter que des informations ne transitent en effet par les nœuds nord-américains ou européens a été exprimée par plusieurs pays, dont les BRICS, qui ont réitéré en 2013 leur soutien à la construction d'un câble reliant par le sud leurs économies, et rééquilibrant la carte actuelle des câbles. Cet exemple parmi d'autres illustre plus largement les débats sur la gouvernance d'Internet, qui concernent également la couche matérielle du cyberespace… dont les câbles sont un élément essentiel.

Il convient ainsi de se demander quelles sont les méthodes utilisées par les Etats pour exercer un contrôle sur les câbles, ainsi que de s'interroger sur les stratégies alternatives mises en place en réaction à ce contrôle. Comment les Etats utilisent-ils ces infrastructures de plus en plus importantes afin de servir des objectifs nationaux? Au regard de la nature des câbles, et des contraintes qu'ils connaissent, quels enjeux représentent-ils et comment sont-ils pris en compte ? Si les câbles sont des infrastructures aussi essentielles que vulnérables, leur contrôle relève d'enjeux économiques, d'influence, et de souveraineté prégnants. Face à ces enjeux, des stratégies ont été mises en place afin de protéger les intérêts nationaux.



Source: Telegeography - Carte des 265 câbles sous-marins en service en 2013

2.1 Des câbles aussi essentiels que vulnérables

Terrestres ou sous-marins, les câbles sont vulnérables et ne constituent pas le seul vecteur pour les communications et les transferts de données.

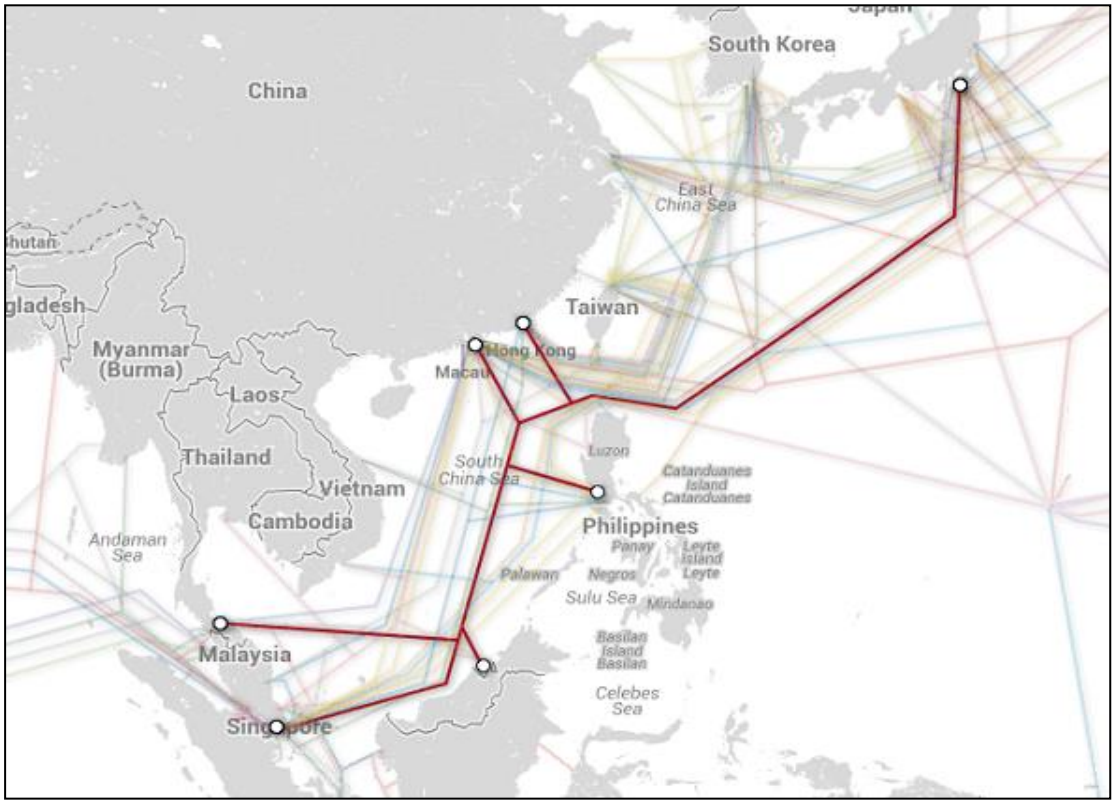
2.1.1 *Rôle et fonctionnement des câbles*

La mise en service du tout premier câble sous-marin, reliant les Etats-Unis et l'Europe date de 1858. Les lignes télégraphiques ont très tôt représenté des enjeux stratégiques de par la possibilité pour un adversaire de couper les communications. Durant la Première Guerre mondiale, le Royaume-Uni bénéficiait d'un réseau de câbles sous-marins très développé qui lui a permis à la fois de maintenir ses communications, et de couper celles de l'Allemagne dans de nombreuses situations.[30]

Les câbles modernes utilisent la fibre optique pour transporter des données numériques incluant les communications téléphoniques, Internet et des transferts de données privées. Ces câbles introduisent un nouveau moyen d'action: si leur coupure peut être dommageable, la quantité croissante de données qu'ils transportent fait de leur contrôle un atout également important.

Les câbles utilisant la fibre optique permettent des échanges de données bien plus rapides que les satellites, réduisant ainsi la latence dans les régions qu'ils connectent. La construction et la pose d'un câble représente un investissement conséquent, qui nécessite généralement la constitution d'un consortium d'opérateurs télécom afin de pouvoir mener le projet à bien. Ce consortium est constitué d'acteurs qui retireront des bénéfices de l'accès au câble, auxquels peuvent s'ajouter de grands groupes d'Internet pour des raisons variées. La construction du câble Asie du Sud-Est - Japon (SJC), qui a coûté 400 millions de dollars pour relier sept pays de la région (Japon, Chine, Philippines, Brunei, Thaïlande, Singapour et Indonésie), a par exemple été financée par un consortium réunissant neuf grands groupes télécom des pays de la région ainsi que le géant américain Google. Le câble a été construit par le fournisseur américain TE SubCom.

[30] Imperial Cable Communications and Strategy, 1870-1914 P. M. Kennedy The English Historical Review http://www.jstor.org/discover/10.2307/563928?uid=3738016&uid=2&uid=4&sid=21103315308633



Le câble sous-marin South-East Asia Japan (SJC)

Source: Telegeography

Les câbles peuvent être terrestres ou sous-marins, en fonction des risques et des routes à suivre. Les câbles sous-marins arrivent dans des stations de contrôle une fois qu'ils atteignent un continent. La gestion des infrastructures en lien avec les câbles est assurée par les membres du consortium ayant participé au projet initial; les coûts restent dans la plupart des cas supportés par le consortium. Les Etats sont en charge de la protection des câbles sur leur territoire et peuvent mettre en place différents moyens afin de remplir cette mission. Ils peuvent cependant décider d'allouer des moyens supplémentaires à la protection des câbles comme nous le verrons par la suite.

La protection des câbles est un élément essentiel du fait de leur exposition aux risques naturels et humains.

2.1.2 *Des infrastructures fragiles et vulnérables*

L'objectif à travers la pose des câbles est de minimiser les dommages qui peuvent leur être infligés par l'activité humaine ou par des catastrophes naturelles. Lorsque cela est possible, ils suivent et se servent d'infrastructures déjà construites telles que le réseau télécom déjà existant (comme c'est le cas en Russie), ou d'autres infrastructures telles que des pipelines.

Les câbles terrestres sont par nature plus exposés aux risques liés à l'activité humaine. Suivant généralement la route d'autres infrastructures énergétiques ou télécom, ils peuvent être victimes de

manière directe ou par ricochet d'opérations de sabotage. Les dommages causés aux câbles peuvent être involontaires: en 2011, une femme géorgienne surnommée "le hacker à la pelle" a endommagé un câble alors qu'elle creusait le sol pour trouver du cuivre. L'Arménie dépendant à 90% de ce câble pour accéder à Internet, le pays s'est trouvé dans l'impossibilité de se connecter pendant les cinq heures qui ont suivi le fameux "coup de pelle". Au-delà des risques liés à l'activité humaine, les câbles terrestres sont également très vulnérables aux catastrophes naturelles telles que les tremblements de terre.

Les câbles sous-marins sont plus difficiles d'accès et donc plus protégés des risques liés à l'activité humaine. Le fait qu'ils soient clairement indiqués sur les cartes et qu'ils ne soient pas protégés les rend néanmoins vulnérables face à des acteurs disposant des moyens nécessaires pour les endommager. En mars 2007, des pirates ont par exemple dérobé onze kilomètres de câbles sous-marins en Asie du Sud-Est, causant d'importants ralentissements d'Internet au Vietnam. Les câbles sous-marins sont également vulnérables aux activités de pêche: les ancres et les filets des navires pouvant les rompre aisément. Un exercice de Cyberdéfense de l'OTAN incluait ainsi dans son scénario le fait que des marins laissent traîner leur ancre sur ordre d'un pays ennemi afin de rompre des câbles au large de la France et du Royaume-Uni, et ainsi créer des coupures d'Internet majeures en France et en Europe. Enfin, les câbles sous-marins sont également vulnérables aux catastrophes naturelles. Les tsunamis et tremblements de terre qui ont eu lieu en Asie ont régulièrement endommagé les câbles, causant d'importantes coupures d'Internet dans certains pays de la région. Parmi ces catastrophes naturelles, un glissement de terrain sous-marin entre Taïwan et les Philippines en 2006 a par exemple endommagé dix-neuf câbles sur les vingt disponibles en Asie du Sud-Est, causant des coupures d'Internet dans la plupart des pays de la région.

2.1.2.1 La constitution de zones de protection

Afin de mieux défendre les câbles, certains pays ont mis en place des zones de protection dans lesquelles le trafic maritime est sous haute surveillance, tandis que des équipes de réparation sont constituées pour intervenir en cas de dommage causés aux câbles. L'Australie a**,** par exemple**,** mis en place trois zones de défense, au large de Sydney et Perth[31], afin de veiller sur les points de rencontres des cinq câbles reliant le pays au reste du réseau mondial. En comparaison, la Nouvelle-Zélande dispose de dix zones de défense pour protéger ses câbles. Le fait que les câbles se rejoignent et forment des nœuds permet de réduire le nombre de zones à surveiller, mais peut également réduire la résilience du réseau national. En décembre 2008, une ancre a coupé les trois câbles au large d'Alexandrie qui transportaient 90% des communications entre l'Europe et l'Asie, causant des pertes de connectivité très importantes dans quatorze pays. L'Inde a perdu 80% de sa connexion à internet suite à cet évènement, et les Maldives 100%. Certaines zones maritimes où de nombreux câbles se

[31] *Australia's vulnerable submarine cables*. Jessica Woodall - Mai 2013

rejoignent font donc l'objet d'une grande vigilance de la part des autorités. Selon Jason Healey[32], le directeur du Cyber Statecraft Initiative of the Atlantic Council, une des zones de protection efficace à l'heure actuelle se trouverait au large de la station de contrôle de Bude, sur la côte britannique. Une tentative de sabotage sur des câbles au large de cette station serait probablement - selon Healey - stoppée du fait de la surveillance mise en place par les autorités maritimes britanniques.

2.1.2.2 La mise en place d'un réseau de câbles plus dense

Un moyen supplémentaire pour prévenir les risques liés aux coupures de câbles est la densification du réseau connectant le pays au reste du monde. Des pays reliés à plusieurs câbles ont de plus grande chance d'éviter les coupures d'Internet totales à l'échelle du pays. Ces *dernières* sont en effet une réalité: depuis janvier 2012, 17 pays ont été affectés à des coupures d'Internet significatives (plus de 90%) selon James Cowie[33].

2.1.3 *Quelles alternatives?*

Les Etats peuvent réduire les risques de ralentissement majeur voire de coupure de leur connexion en multipliant les câbles connectant leurs pays à Internet, améliorant également le temps de réaction des équipes dédiées à la réparation de ces infrastructures. Des alternatives aux câbles sont également à l'étude.

Les satellites permettent à un pays d'avoir accès à Internet sans passer par les câbles, mais la distance à laquelle ils se trouvent provoque une latence importante et ne permet pas d'avoir le même volume de bande passante qu'avec les câbles. De plus, la mise en place d'un satellite, ou ne serait-ce que son utilisation représente un coût plus important que celle des câbles. Si cette solution est bien plus onéreuse et bien moins efficace qu'un câble, elle permet néanmoins de connecter certaines régions du monde trop difficiles d'accès. Des améliorations ont récemment été faites pour augmenter la vitesse à laquelle les données sont transmises par les satellites, réduisant largement la latence mais ne permettant toujours pas d'égaler la vitesse de transmission des données permise par un câble, du fait encore une fois de la distance à laquelle se trouvent les satellites.

Plusieurs initiatives sont en développement pour résoudre ce problème de latence. Elles consistent en la mise en place de dispositifs remplissant le rôle de satellite mais volant à plus basse altitude. La *Defense Advanced Research Projects Agency* (DARPA) américaine, entre autres acteurs publics et privés, travaille à la construction de drones volant à haute altitude et disposant d'équipements leur permettant de jouer le même rôle qu'un satellite de communication. En se servant de l'énergie solaire, ces drones pourraient rester de très longues périodes en vol et remplir le rôle d'un satellite de communication tout en permettant d'éviter les coûts élevés de conception et de mise sur orbite.

---

[32] http://www.nationaljournal.com/tech/how-do-you-protect-undersea-internet-cables-anyway-20130509
[33] *Internet Infrastructure: Virtual meets Reality.* James Cowie, Renesys Corporation - Septembre 2013

La position de ces drones, plus proche de la terre, réduirait également la latence occasionnée par le temps de transmission des données. Dans le cadre de son projet "*Loon for all*", Google a également développé des ballons permettant aux zones ne disposant pas d'un accès à Internet du fait de leur position géographique, du niveau de développement du pays ou suite à une catastrophe naturelle, de bénéficier d'un accès à Internet. Si le concept est relativement similaire aux drones, les ballons se serviraient des courants aériens pour rester au-dessus de la zone désignée.

Ces alternatives ne sont qu'à l'état de projet et ne permettent pas d'égaler la vitesse à laquelle les données sont transférées à travers les câbles - qui connaissent également des améliorations technologiques. La vulnérabilité des câbles représente donc un défi majeur du fait des enjeux économiques et politiques croissants qu'ils représentent.

2.2 Le contrôle des câbles: un enjeu à l'importance croissante

Les câbles représentent un enjeu croissant pour les Etats. Leur protection représente à la fois un enjeu économique et de garantie de la souveraineté, tandis que leur contrôle permet d'influencer ou d'exercer une pression sur des Etats tiers par différents moyens.

2.2.1 *Un enjeu économique crucial*

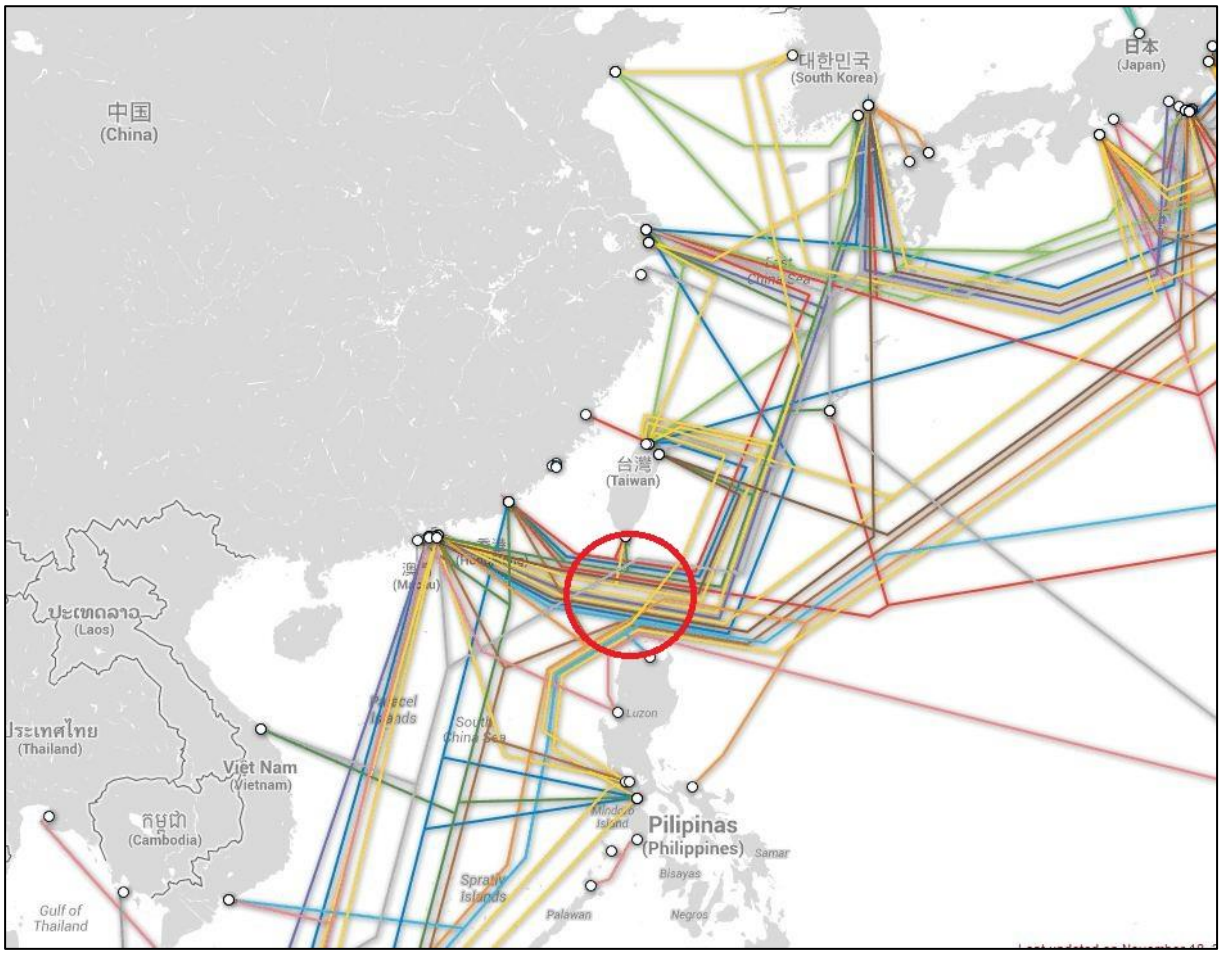
Les câbles sont le premier vecteur d'échange d'informations au niveau international. Ils sont essentiels au bon fonctionnement de l'économie dans des pays de plus en plus dépendants des Nouvelles Technologies de l'Information et des Communications (NTIC). Les dommages causés aux câbles peuvent affecter le fonctionnement de l'économie des pays touchés, et représenter des pertes très importantes pour les Etats.

Au regard des enjeux économiques liés aux câbles, l'Australie a déclaré que les cinq câbles sous-marins qui relient le pays au réseau mondial représentent un "enjeu vital", une coupure d'Internet lui faisant perdre 152 millions[34] par jour jusqu'à rétablissement de la connexion selon les estimations de l'Asia Pacific Economic Cooperation (APEC)[35].

Le tremblement de terre Hengchun de 2006 a endommagé sept câbles en dix-neuf points dans le voisinage du détroit de Luzon, causant d'importantes pertes de connectivité en Asie du Sud-Est. Les échanges de données entre acteurs économiques de la région se sont retrouvés en conséquence drastiquement réduits, pénalisant les économies des pays touchés par les pertes de connectivité. Les

[34] *Australia's vulnerable submarine cables*. Jessica Woodall - Mai 2013
[35] *Economic Impact of Submarine Cable Disruption*. Asia Pacific Economic Cooperation (APEC) http://publications.apec.org/publication-detail.php?pub_id=1382

marchés financiers et le commerce dans sa globalité ont été affectés par l'impossibilité d'accéder aux boîtes mails, aux services de banque en ligne ou de réservation de transports. La réparation des câbles a mobilisé 11 navires pendant 49 jours avant un retour à la normale[36]. Les pertes économiques liées au tremblement de terre ont été très importantes: une étude en Chine a montré que 97% des internautes chinois ont connu des difficultés à accéder à des sites internet étrangers, tandis que 57% d'entre eux estiment que ces coupures ont affecté négativement leur quotidien et leur travail[37].



Le détroit de Luzon, lieu de passage de nombreux câbles sous-marins

Source: Telegeography

[36]Critical Infrastructure Submarine Telecommunications Cables, ICPC, 2010
[37]Bebenbeschert Rückfallins Telefonzeitalter, Nordkurier, 2006

2.2.2 *Un moyen d'influence et de renseignement*

L'accès aux câbles est un enjeu pour les agences de renseignement, du fait de la possibilité d'installer des dispositifs d'interception des données transitant par ce biais. Un câble traversant le territoire national permet**,** en effet**,** à ces services de renseignement de collecter un très grand nombre de données tout en bénéficiant du cadre juridique national. Il est possible de collecter les données afin de les analyser en temps réel ou de les stocker pour une étude ultérieure. En 2013, plusieurs révélations ont permis de prendre la mesure de la surveillance exercée par les services de renseignement à partir des câbles.

Si la volonté de pouvoir accéder aux réseaux de communication utilisés par d'autres Etats n'est pas nouvelle (la première mise sur écoute d'un câble sous-marin par la NSA datant par exemple de 1971 avec l'opération Ivy Bell[38]), elle est aujourd'hui de plus en plus visible et nécessaire du fait de l'importance croissante des câbles. A ce titre, l'affaire Snowden a montré l'ampleur avec laquelle des services de renseignement britanniques et américains, respectivement le *Governement Communications Headquarter (GCHQ)* et la *National Security Agency (NSA)*, pratiquaient cette méthode de collecte de données dite "Upstream". La station d'atterrissage des câbles de Bude, sur la côte britannique, accueille par exemple six câbles par lesquels transitent 10% du trafic international et offrent ainsi aux services de renseignement britanniques un accès stratégique à une très grande quantité de données. Au total, 49 des 265 câbles sous-marins en service dans le monde transitent par le territoire britannique, qui possède à lui seul 71 stations de contrôle des câbles au sein desquelles il est possible d'installer des dispositifs de collecte des données[39]. Les Etats-Unis bénéficient d'accords de partage du renseignement avec le Canada, l'Australie, le Royaume-Uni et la Nouvelle Zélande dans le cadre des "Five Eyes"[40],et accèdent à des données collectées sur de nombreux câbles de par le monde grâce à leurs alliés simples partenaires.

Parmi ces partenaires, l'*Australian Signals Directorate* bénéficie d'accords de renseignement avec Singapour pour collecter les données transitant par le câble SEA-ME-WE-3 long de 39 000 kilomètres à travers l'Asie, le Moyen-Orient et l'Europe. Le gouvernement de Singapour possède en effet l'opérateur télécom SingTel qui fait partie du consortium ayant permis la construction du câble, et contrôlant ce dernier sur le territoire de Singapour. C'est par le biais de cet opérateur que les services

---

[38] Ivy Bell le nom une opération menée en 1971 par la CIA et la NSA dans le but de mettre sur écoute un câble sous-marin utilisé par l'URSS pour des communications confidentielles. Le sous-marin USS Halibut, modifié pour l'opération, a permis à des plongeurs de placer un dispositif d'écoute qui enregistrait toutes les communications et se décrochait automatiquement du câble dans le cas où celui-ci était relevé pour réparation. L'opération fut un succès et plusieurs autres dispositifs furent installés à l'aide de cinq autres sous-marins. Le matériel d'écoute était construit par AT&T et Bell Laboratories.

[39] *Les câbles sous-marins, clé de voûte de la cyber surveillance*. Maxime Vaudano, Le Monde, 23 août 2013

[40] "Five Eyes" renvoie au traité UKUSA secrètement signé entre les Etats-Unis et le Royaume-Uni en 1946 afin de mettre en place une collaboration en matière de renseignement électromagnétique. Le Canada, la Nouvelle-Zélande et l'Australie ont rejoint ce traité, les cinq pays formant aujourd'hui les "Five Eyes" (cinq yeux).

de renseignement australiens et Singapouriens ont accès aux données transitant sur un câble majeur.

Les dispositifs d'interception installés sur les câbles peuvent être très difficiles à détecter par les tiers. Ils n'occasionnent en effet que très peu de latence du fait de leur installation directe sur le câble. Ces dispositifs peuvent être des sondes installées sur des nœuds majeurs de câbles, généralement dans les stations de contrôle où les câbles sous-marins atterrissent. Ce procédé peut se faire particulièrement aisément si la station est située sur le territoire national ou sur celui d'un pays avec qui des accords de partage du renseignement d'origine électromagnétique ont été mis en place. A défaut de pouvoir placer des sondes dans ces stations, il est possible d'installer des dispositifs d'écoute à même le câble. A l'image des dispositifs utilisés par la NSA lors de la Guerre Froide et suite à l'opération Ivy Bell, ceux-ci peuvent être très difficiles à détecter et sont mis en place, dans le cas des Etats-Unis, par des sous-marins spécialement équipés dans ce but, comme nous le verrons par la suite[41]. De nombreux Etats ont adopté des cadres juridiques favorables aux agences de renseignement, qui peuvent obliger les opérateurs télécom à leur fournir un accès aux données transitant sur les câbles.

2.2.3 *La nécessité de garantir sa souveraineté*

L'accès aux câbles et la constitution d'un réseau de câbles diversifié ne relèvent pas seulement d'une préoccupation économique, mais également d'un choix stratégique. Un pays ne possédant qu'un seul câble, qui transite par un Etat tiers, s'expose à plusieurs dangers: non seulement il risque de permettre à l'Etat tiers d'accéder à une très grande partie des données échangées sur le territoire national et avec l'étranger, mais il s'expose également à des pressions.

Les câbles comme moyens de pression

La capacité d'un Etat à diversifier ses accès à internet et à choisir les routes empruntées par les câbles qui le relient au réseau mondial représentent un atout permettant de s'émanciper de possibles pressions exercées par des tiers. Si l'exemple cité plus tôt de la coupure d'Internet en Arménie suite à une faute humaine en Géorgie relève d'un accident, d'autres coupures peuvent être intentionnelles. En mars 2013, les forces navales égyptiennes ont arrêté trois plongeurs qui tentaient d'endommager les câbles sous-marins au large du port d'Alexandrie. Cette arrestation a fait suite à plusieurs coupures qui avaient eu lieu sur plusieurs câbles au même endroit la même semaine, causant d'importants ralentissements dans l'accès à internet de plusieurs pays. Si cet acte de sabotage n'a pas été lié à la volonté d'un Etat, cela montre que des actions de sabotage sur les câbles sont réalisables et représentent une menace pour les Etats n'étant relié que par peu de câbles, ou par des câbles ne se rejoignant qu'en un point au large du pays.

[41] http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=1&

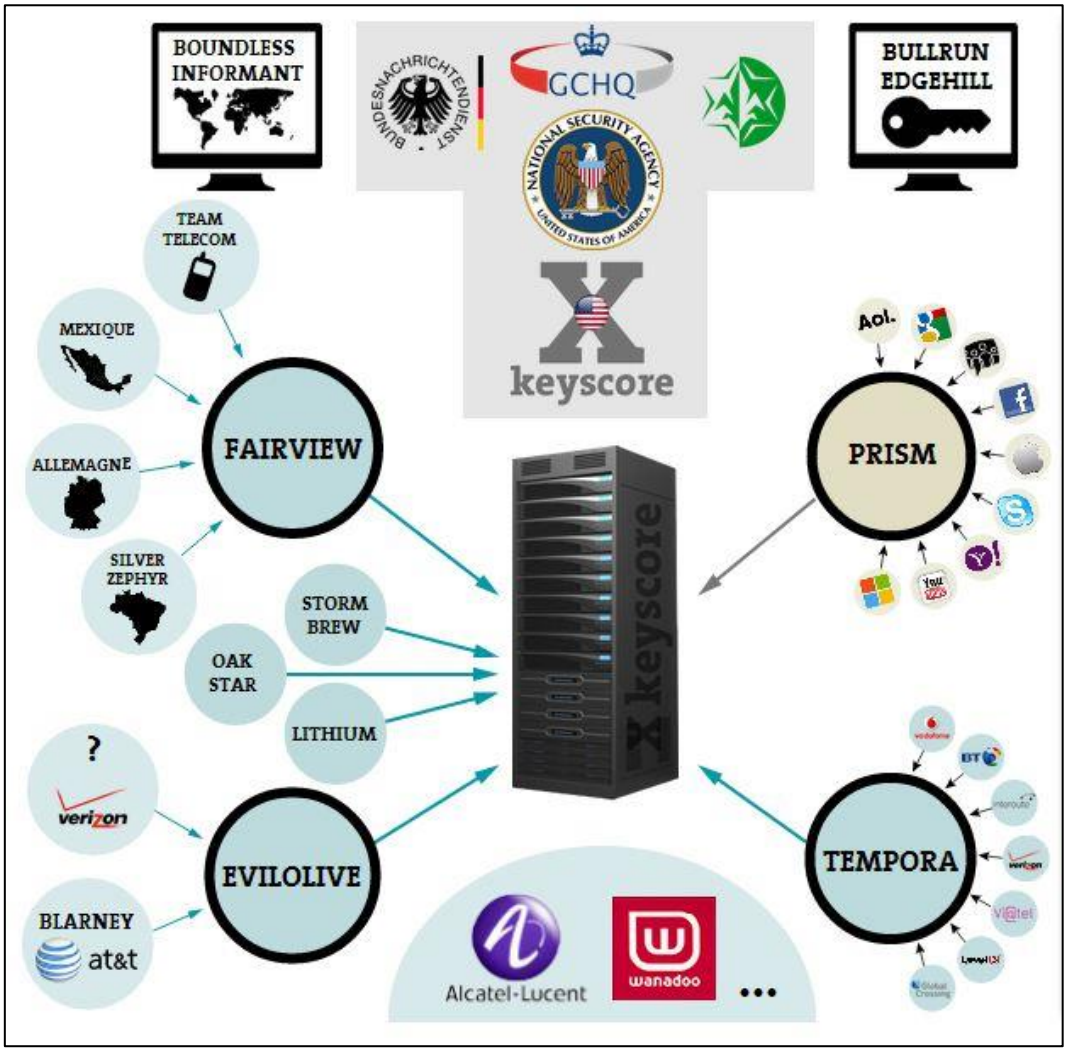
Un Etat peut exercer des pressions sur un autre à travers le processus de construction d'un câble. Comme nous l'avons vu, celle-ci requiert des investissements importants généralement effectués par un consortium d'opérateurs télécom des pays bénéficiant de la construction du câble. De par son influence et sa puissance économique, un pays peut influer sur la décision de construire un câble dans sa zone géographique, ainsi que sur le tracé que celui-ci devra suivre. C'est le cas des Etats-Unis qui, en vertu d'un embargo contre Cuba mis en place depuis 1960, ont bloqué les projets de câble qui aurait permis de relier l'île au reste du monde par d'autres moyens que les liaisons satellites. En 2011, Cuba a malgré tout réussi à accéder à un câble, baptisé ALBA-1, qui l'a relié au Venezuela et en 2013 à la Jamaïque.

2.2.4 *Lutter contre la surveillance de masse*

Les câbles sont un moyen pour les Etats d'accéder à une grande quantité de données. La construction d'un câble a donc un rôle stratégique car son tracé va faciliter ou rendre plus difficile l'accès au câble par certains Etats. L'affaire Snowden en 2013 a montré l'étendue des moyens et le fonctionnement des programmes mis en place par les Etats-Unis pour mettre en place une surveillance de masse à partir câbles auxquels ils ont accès. La National Security Agency dispose de deux méthodes pour collecter les données. La première est basée sur la collecte de données "Downstream", c'est-à-dire directement dans les serveurs des entreprises qui les stockent. La seconde méthode est "Upstream", et a lieu lors du transit des données par le biais de vecteurs auxquels les Etats-Unis ou leurs alliés ont accès.

Source: Washington Post[42]

Elle se concentre en grande partie sur les câbles du fait de l'énorme quantité de données qu'ils transportent. Les révélations de l'affaire Snowden ont montré que la collecte de données "Upstream" se fait grâce à plusieurs programmes:



Organisation programmes de collecte de données de la NSA

Source: Le Monde[43]

[42] http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html

[43] http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html

Evilolive: programme qui a pour but de collecter toutes les métadonnées[44] des communications circulant dans les réseaux de trois grands opérateurs télécoms américains. Parmi ces grands opérateurs se trouvent AT&T, et possiblement Verizon[45]. Le programme se concentre donc sur la collecte de métadonnées grâce à des sondes placées avec la coopération des grands opérateurs télécoms.

Tempora: second programme de collecte de données datant de 2011 et mené par le GCHQ. Il garantit aux services britanniques un accès illimité aux câbles de sept grandes entreprises télécoms mondiales: British Telecom, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel et Interoute. Des systèmes d'écoute ont été installés sur plus de 200 câbles appartenant à ces entreprises, permettant aux services britanniques d'accéder à 21 pétaoctets de données par jour et de les partager avec son allié américain. Le Royaume-Uni, de par sa position centrale dans le réseau des câbles mondial, représente un atout stratégique pour les Etats-Unis qui ont financé le développement des infrastructures britanniques dédiées. Le programme Tempora coûterait 117 millions de dollars sur trois ans à la NSA, dont 17,8[46] millions auraient été alloués à la rénovation de la base du GCHQ de Bude. Cette base, créée dans le cadre du réseau Echelon, est à proximité de la station de contrôle de Bude par laquelle transitent sept câbles majeurs.

La base du GCHQ à Bude

Source: Public Intelligence[47]

[44] Les métadonnées sont l'ensemble des données qui accompagnent le contenu des communications ou des messages. Elles permettent de savoir la date, l'heure, la location, et le nom de l'interlocuteur en cas de communication téléphonique. Pour les messages circulant sur internet, ces données peuvent également être accessibles ainsi que le nom du site visité.

[45] http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

[46] *Les câbles sous-marins, clé de voûte de la cyber surveillance*. Maxime Vaudano, Le Monde, 23 août 2013

[47] http://publicintelligence.net/page/9/?s=cell

Les révélations de l'affaire Snowden ont ainsi précipité une prise de conscience des capacités d'espionnage permises par les Technologies de l'Information et de Communication (TIC). Le Brésil a réagi vivement en septembre 2013 aux révélations de la mise sur écoute des téléphones de la Présidente Dilma Rousseff ainsi que de ceux de ses collaborateurs. L'espionnage économique fait à l'encontre de l'entreprise pétrolière Petrobras a été dénoncé comme une "*violation de la souveraineté*" brésilienne, menant les membres du gouvernement brésiliens et argentins à travailler de concert à la mise en place d'un Internet à l'abri de l'espionnage de la National Security Agency (NSA). Plusieurs mesures ont été entreprises dans cette optique. La Présidente Dilma Rousseff a demandé le 11 septembre de traiter avec une "urgence constitutionnelle" le vote du "Marco Civil da Internet", un texte qui a pour but de garantir les droits des citoyens brésiliens dans leur usage d'Internet[48]. Elle a aussi exprimé sa volonté de contraindre les entreprises ayant en leur possession les données des citoyens brésiliens à stocker ses données sur le territoire national.

Enfin, parmi les mesures qui permettraient de réduire la surveillance américaine, la remise en question d'une structure des câbles trop centrée sur les Etats-Unis et l'Europe de l'ouest est apparue comme une préoccupation importante. La mise en place d'un câble pour les BRICS est un des projets qui permettrait à la Chine, la Russie, le Brésil, l'Afrique du Sud et l'Inde de communiquer sans que les données ne passent par le territoire des Etats-Unis ou du Royaume-Uni.

Les enjeux liés aux câbles sont donc importants. Alors que leur bon fonctionnement est vital pour la plupart des économies, la nécessité de développer un réseau diversifié tout en influant sur les routes empruntées par les câbles apparaît comme une nécessité pour la souveraineté des Etats. Les rapports de pouvoir se reflètent ainsi dans le trajet des câbles et pourraient être de plus en plus prégnants dans les projets de construction en cours ou à venir. De ce fait, certains gouvernements ont développé des moyens et de véritables stratégies afin de garantir l'intérêt national dans le processus de construction et de gestion des câbles.

2.3 Stratégies nationales et moyens dédiés au contrôle des câbles

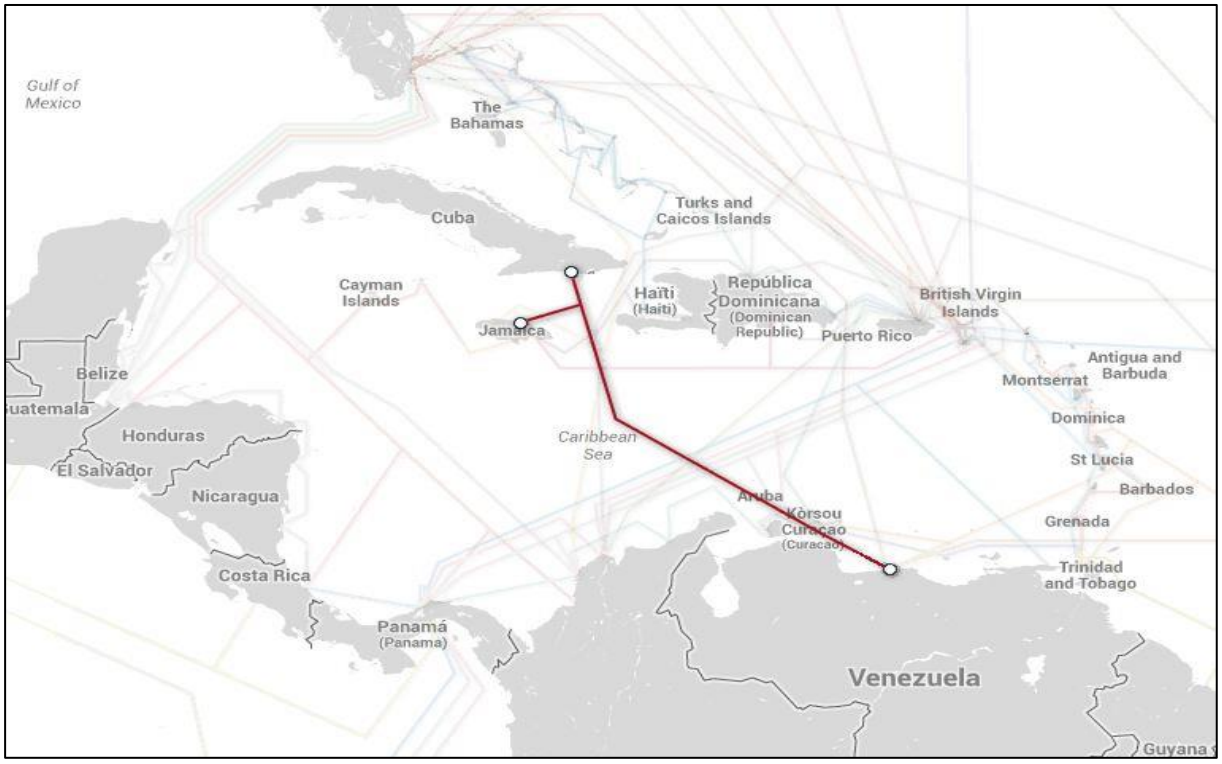
Les câbles sont des infrastructures cruciales et vulnérables, mais également un atout pour tout Etat capable d'influencer leur construction et de les contrôler. Si ces derniers disposent ni des mêmes moyens d'action, ni du même niveau de conscience des enjeux, nombre d'entre eux ont développé à leur échelle des stratégies afin d'utiliser les câbles à leurs propres fins. Alors que la domination américaine est permise par des atouts majeurs, des initiatives sont prises pour développer des câbles alternatifs.

[48] http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html

2.3.1 *ALBA-1 : le câble "anti-impérialiste"*

La construction d'un câble peut être le moyen de se libérer des pressions exercées par un Etat tiers. C'est la stratégie de Cuba à travers la construction du câble ALBA - 1 reliant le pays au Venezuela.

En 2007, les opérateurs télécom cubains et vénézuéliens ont joint leurs forces pour construire le premier câble reliant Cuba au réseau de câbles mondial. Ce projet, entrepris pour "*briser le blocus des communications imposé par les Etats-Unis*", avait pour but d'améliorer significativement (par un facteur 3000) la vitesse de navigation sur internet à Cuba. A cause d'un embargo mis en place par les Etats-Unis en 1960, Cuba avait dû se reposer sur trois satellites pour son accès à Internet, et ce malgré le fait qu'un des nœuds de câble les plus importants se trouve à 32 kilomètres de l'île, au large de Miami. La mise en service du câble en 2011, et son extension à la Jamaïque en 2013, ont amélioré l'accès à Internet de Cuba et permis son désenclavement progressif malgré les pressions exercées par les Etats-Unis.



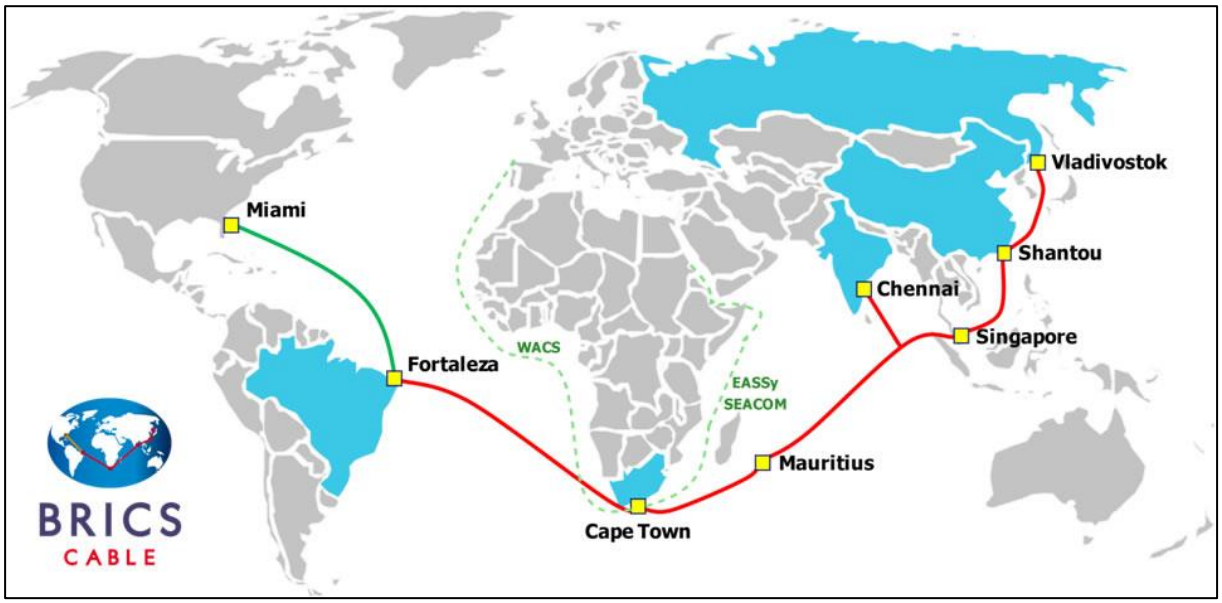
Le câble ALBA-1 en 2013

Source: Telegeography

2.3.2 *Le câble BRICS contre le réseau américano-centré*

La construction d'un câble peut également se faire dans le but de limiter les opérations d'espionnage pratiquées par des Etats tiers. C'est la stratégie des BRICS à travers la construction d'un câble qui devrait éviter de passer par les plaque-tournantes du réseau mondial que sont l'Amérique du Nord et l'Europe.

Les révélations sur la collecte de donnée "upstream" de Washington et de ses alliés a accéléré la prise de conscience d'un réseau de câbles trop centré sur l'Europe et les Etats-Unis, facilitant grandement les opérations d'espionnage des pays par lesquels les câbles transitent. L'espionnage économique de l'entreprise pétrolière brésilienne Petrobras a été l'élément déclencheur d'une vive fronde en Amérique Latine contre l'espionnage américain. Le projet de câble BRICS a pour but de rééquilibrer le réseau des câbles mondial en proposant un câble "sud" reliant le Brésil, l'Afrique du Sud, la Chine, la Russie et l'Inde en contournant les nœuds de câbles d'Amérique du Nord et d'Europe.



Le projet de câble reliant les BRICS

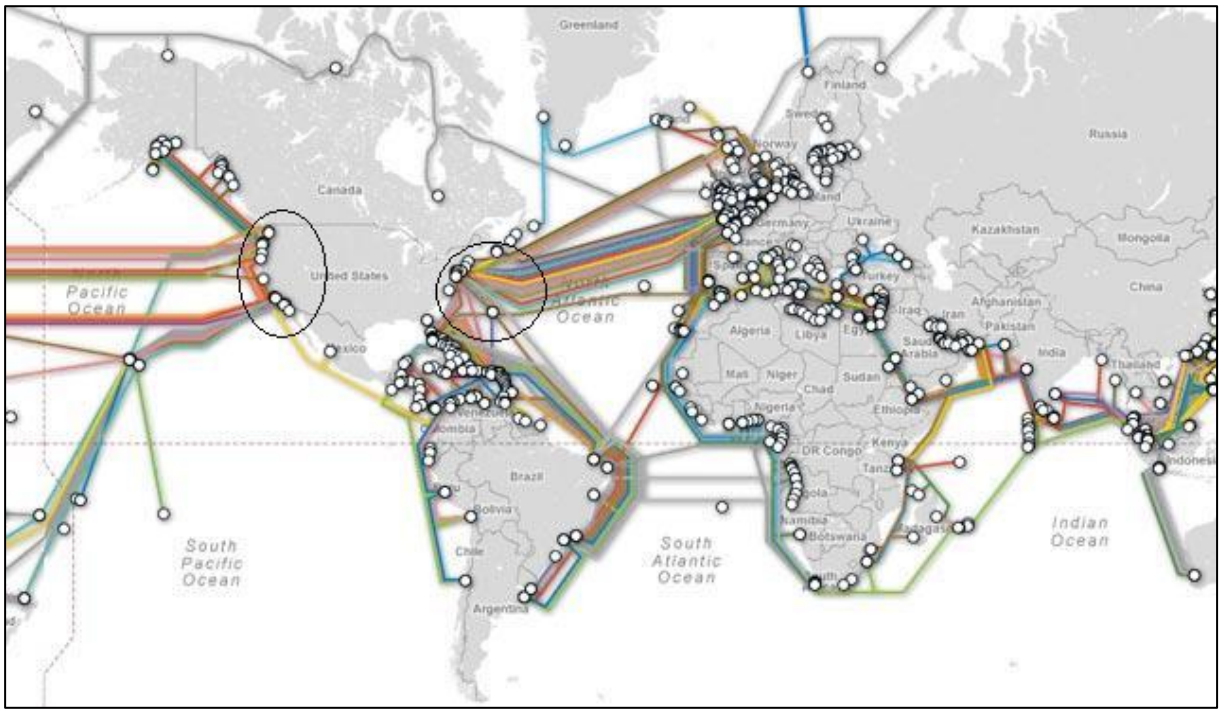
Source: BRICSCable.com

Si les objectifs du câble sont clairs, son tracé soulève de nombreuses interrogations. Par exemple, le trajet du câble devrait le faire passer par une station de contrôle sur l'île d'Ascension appartenant au Royaume-Uni. Cette île, réputée pour avoir "plus d'antennes que de résidents", accueille une base aérienne américaine ainsi qu'une station d'interception des communications du Governement Communications Headquarter (GCHQ) britannique. Selon les documents fournis par Edward Snowden, c'est à partir de cette île que les opérations d'espionnage de l'entreprise Petrobras auraient été menées. Le câble BRICS devrait également relier la ville de Miami à une de ses extrémités, et modifier sa route initiale pour passer par l'île de Sainte Hélène, jumelle également britannique de l'île d'Ascension. La volonté des BRICS de contourner le réseau des câbles centré sur les Etats-Unis et le Royaume-Uni ne devrait finalement pas être entièrement mise en application.

2.3.3 *Etats-Unis: une forme de doctrine Monroe des câbles?*

La carte des câbles sous-marins en service est révélatrice de la domination des Etats-Unis sur le continent américain. La quasi-totalité des câbles reliant le continent américain aux autres continents

passe par des stations de contrôle situées sur le territoire américain. Les câbles en direction de l'Asie du Sud-Est par l'océan Pacifique passent tous par les stations de contrôle de la côte Ouest américaine ainsi que par Hawaï. A l'Est, seul un câble intercontinental ne passe pas par le territoire américain. Celui-ci relie l'Amérique Latine à l'Afrique en passant par l'Océan Atlantique Ainsi, la quasi-totalité des données transitant par les câbles qui relient le continent américain au reste du monde passe donc par le territoire des Etats-Unis ou du Royaume-Uni. La position centrale des Etats-Unis dans le trajet des câbles quittant le continent américain représente un atout majeur permettant la mise en place d'une surveillance de masse des communications et des échanges de données.

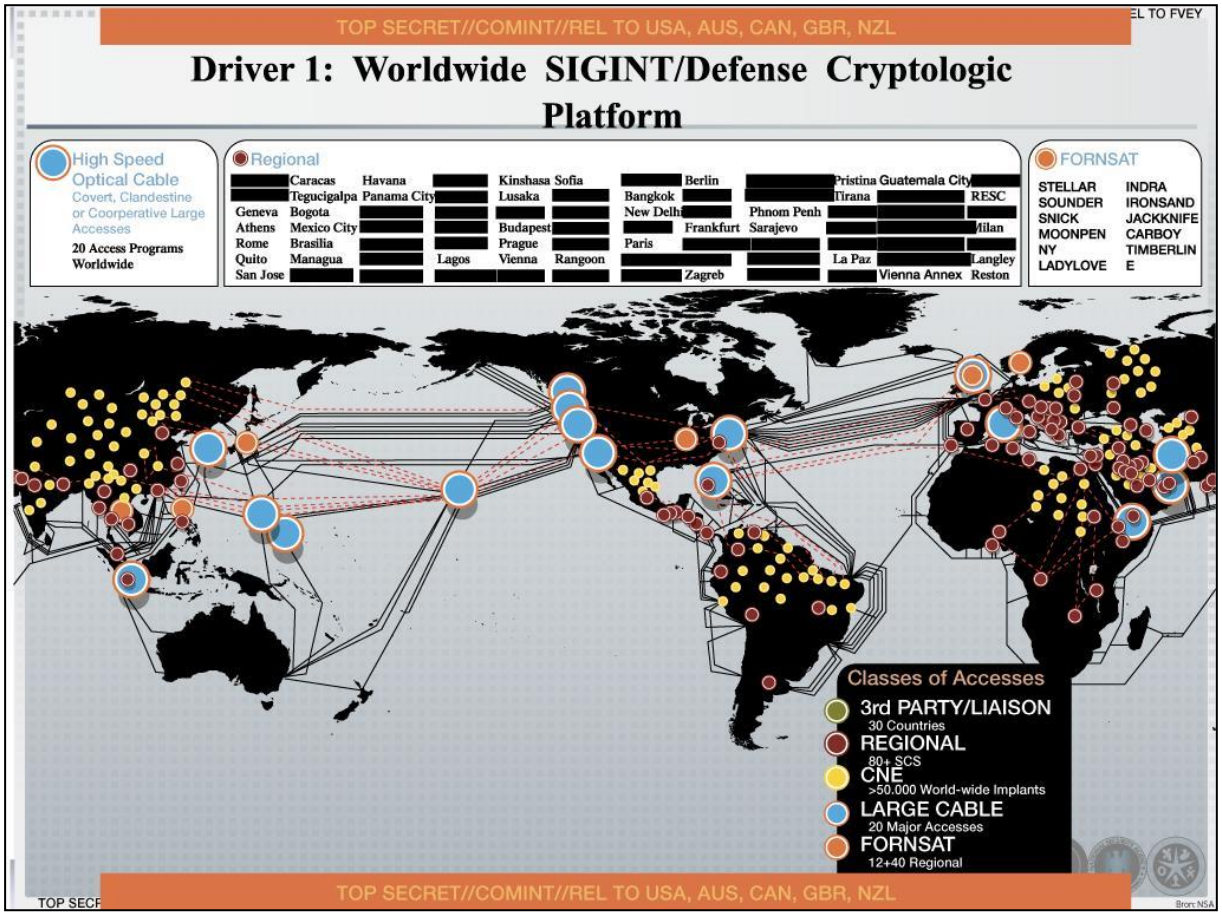


La doctrine Monroe des câbles?

Source: Telegeography

La localisation des dispositifs américains de collecte de renseignement à partir des câbles est ici particulièrement révélatrice de l'avantage stratégique des Etats-Unis. Il est en effet possible de constater que, si les Etats-Unis disposent de moyens de collecte à partir de câbles sur tous les continents, ceux-ci sont concentrés sur les côtes nationales en ce qui concerne le continent américain. La quasi-totalité des câbles connectant le continent américain au reste du monde transitant par le territoire des Etats-Unis, la NSA peut récupérer toutes les données entrant et sortant du continent américain par les câbles depuis le territoire national. Elle bénéficie de nombreux avantages dont le fait de bénéficier d'un cadre juridique favorable à ses actions, sans s'exposer aux risques liés à des opérations en dehors du territoire national. Le cadre juridique autorisant la surveillance à partir des câbles est le *Foreign Intelligence Surveillance Act* (FISA), amendé en 2008 afin de permettre au gouvernement américain d'espionner les communications des étrangers à l'étranger. Il autorise la collecte de données sur les communications étrangères ou entre un citoyen

américain et un étranger. Il a été étendu jusqu'en 2017 par le Sénat américain, et spécifie que l'espionnage ne doit pas viser intentionnellement un citoyen américain ou une personne située aux Etats-Unis, et ne doit pas aller à l'encontre du quatrième amendement de la constitution des Etats-Unis qui protège la vie privée des citoyens. L'autorité de contrôle est la Foreign Intelligence Surveillance Court, qui délivre des mandats de trois mois autorisant les opérations de surveillance menées par les services américains. Le mandat actuel a été renouvelé par la FISC début 2014.



Les Etats-Unis disposent de moyens de collecte des données sur de nombreux "nœuds" de câbles stratégiques (en bleu sur la carte)

Source: NRC[49]

Les Etats-Unis sont également en mesure de collecter des données sur les "nœuds" principaux de câbles dans le monde, grâce à des opérations clandestines ou la coopération des autorités nationales. Si les opérations clandestines ne sont pas référencées dans les documents, il convient de noter que les Etats-Unis disposent par exemple de sous-marins équipés pour réaliser des écoutes à

[49] http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

partir des câbles sous-marins. C'est le cas du sous-marin USS Jimmy Carter qui fut modifié en 2001 pour pouvoir réaliser des écoutes à l'image de son prédécesseur, l'USS Pache[50]. Des dispositifs autonomes de collecte de données peuvent aussi être installés à même le câble sur les fonds marins, tel que cela fut fait lors de l'opération Ivy Bell détaillée plus haut.

Plusieurs pays ont en revanche accepté de collaborer avec les Etats-Unis dans le cadre des accords UKUSA élargis. Ainsi, si le Canada, le Royaume-Uni, les Etats-Unis, l'Australie et la Nouvelle-Zélande coopèrent dans la collecte de renseignement d'origine électromagnétique (SIGINT), notamment par le biais d'interception des communications (COMINT), d'autres pays tiers se sont associés aux "Five Eyes". Singapour est par exemple un des pays tiers associé aux programmes, en collaborant avec l'Australian Signals Directorate pour collecter des données sur les câbles dans sa zone géographique.

Washington dispose également de plusieurs atouts lui permettant de continuer à influer sur le tracé des câbles et de conserver le contrôle de ceux existant.

2.3.3.1 Une puissance économique facilitant le contrôle des câbles

Le premier atout est sans nul doute la puissance d'une industrie spécialisée et dynamique dans le domaine des Technologies de l'Information et des Communication à l'image des géants d'Internet que sont Google, Apple, Amazon et Microsoft. Les grands groupes télécom américains tels que Level 3, Verizon, AT&T, ont contribué à la construction de nombreux câbles qu'ils possèdent aujourd'hui en partie. Toutes ces grandes entreprises ont les moyens financiers et le savoir-faire nécessaire pour faire partie des consortiums et peser dans la construction des câbles de par le monde. Si les sept entreprises du programme Tempora sont forcées de collaborer avec les autorités britanniques dans le cadre du Regulation of Investigatory Powers Act en vigueur depuis l'année 2000[51], les trois entreprises faisant partie du programme Evilolive agissent sur la base du volontariat et reçoivent des compensations financières de la part du gouvernement américain selon un rapport de 2009 publié par le Guardian[52]. Dans le cadre du programme baptisé Blarney, l'entreprise américaine AT&T fournit, depuis une date antérieure à 2001, les métadonnées des communications téléphoniques et internet passant par son réseau à la NSA. Ce programme coûte 50 millions par an au gouvernement américain selon le "budget noir" publié par le Washington Post[53].

---

[50] http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0
[51] http://www.legislation.gov.uk/ukpga/2000/23/contents
[52] http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection
[53] http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html

2.3.3.2 Un cadre juridique spécifique lié aux services de renseignement

Le second atout américain est la "Team Telecom". Cette équipe, composée de juristes dépendant du FBI et du Department of Justice (DOJ), a pour objectif d'empêcher de grands groupes ou des gouvernements étrangers de prendre le contrôle de câbles et mettre en péril les programmes de collecte de données "upstream" de la NSA. Elle intervient de deux manières pour atteindre cet objectif.

La Team Telecom a tout d'abord mis en place en 2003 le premier "Network Security Agreement" avec l'entreprise Global Crossing, accord qui est devenu un modèle imposé par la suite à d'autres entreprises américaines. Alors que la concurrence se fait de plus en plus forte pour la construction et le contrôle des câbles, cet accord contraint les entreprises américaines à mettre en place un système permettant aux agences de renseignement d'accéder aux données circulant sur les câbles lorsqu'elles le demandent. La Team Telecom intervient également dans les négociations pour la construction de câbles, ou le rachat de ceux existant par des entreprises étrangères, selon une procédure précise. Lors des négociations, c'est la Federal Communications Commission (FCC) qui doit accorder une licence autorisant le début du projet. Cette dernière peut décider de se prononcer après un long délai, afin de permettre aux juristes de la Team Telecom de mettre en place des accords de sécurité contraignants avec les parties prenantes du projet. Si ces accords ne sont pas acceptés par les entreprises étrangères, la FCC peut alors refuser d'accorder la licence nécessaire.

L'exemple le plus probant de l'action de la Team Telecom est l'accord sur Global Crossing de 2003. En 2002, Global Crossing possédait un réseau de câbles à fibre optique reliant 27 pays et quatre continents, mais était proche de la faillite avec douze milliards de dollars de dettes. Deux entreprises, l'une de Singapour et l'autre de Hong-Kong, ont passé un accord pour acquérir la majeure partie de l'entreprise américaine. Cette initiative a immédiatement été perçue comme une menace pour les programmes de surveillance américains et, sous la pression de la Team Telecom, l'entreprise de Hong-Kong s'est rapidement retirée des négociations. L'entreprise Singapourienne restante a dû accepter de nombreuses conditions posées par la Team Telecom avant de pouvoir procéder au rachat de Global Crossing: une filiale dédiée à la gestion des câbles sous-marins devait être créée, avec un comité exécutif à moitié composé de nationaux américains habilités top secret. Un "Network Operation Center" a également été mis en place sur le sol américain, et devait pouvoir être visité avec un préavis de 30 minutes par des représentants du gouvernement.

2.4 Conclusion

Si les câbles sont très vulnérables aux risques naturels et humains, ils représentent aujourd'hui des éléments essentiels de la couche physique du cyberespace. Ils permettent la transmission de très grande quantité de données à une vitesse qui n'est pas encore égalée par les autres vecteurs existants. Le fait qu'ils soient à la fois vulnérables et au cœur d'enjeux de plus en plus cruciaux

nécessite le développement de stratégies afin de sauvegarder les intérêts nationaux. Même si les États Unis sont au cœur du réseau des câbles à l'échelle mondiale, la forte exposition médiatique dont la National Security Agency a fait l'objet a précipité une prise de conscience des enjeux parmi de nombreux pays ainsi que la formulation de premières stratégies visant à présenter une alternative échappant au contrôle américain. Ces stratégies en direction de la couche matérielle du cyberespace viennent aujourd'hui compléter celles mises en place plus globalement par les Etats pour s'assurer le contrôle des trois couches matérielles, logicielles et sémantiques dans lesquelles la prépondérance américaine est mise en lumière.

Ces stratégies alternatives liées aux câbles peuvent ne pas aboutir, notamment du fait des moyens développés par les Etats-Unis pour maintenir leur domination, mais elles témoignent d'une volonté de remettre en question l'équilibre actuel de la couche matérielle du cyberespace.