Le fonctionnement d’Internet ne tient qu’à (presque) un fil

	Le fonctionnement d’Internet ne tient qu’à (presque) un fil

L'imaginaire populaire associe souvent Internet aux satellites, mais 99,8 % du trafic intercontinental passe par les 366 câbles sous-marins répartis sur la planète. « Grâce à la fibre optique, les capacités de ces câbles sont des millions de fois supérieures à ce que nous savons faire avec les satellites ».

Rien n'est plus facile que de couper Internet : il suffit de sectionner des câbles. Ils sont simplement enterrés, voire posés sur le fond des océans.

La câbles sous marins ont pris une importance prépondérante pour l'acheminement des connexions internet. Se sont des ressources de plus en plus essentielles et toutes perturbations provoqueraient de très importantes conséquences.

Selon le New York Times les Russes joueraient actuellement avec les nerfs des autorités américaines en laissant des navires très proches de ces câbles sous-marins et n'hésitant pas à frôler ces derniers… Or, il faut savoir que non seulement ces câbles sont très difficile à protégés du fait de leur longueur de plusieurs milliers de kilomètres mais aussi bizarre que cela puisse paraitre, aucune loi maritime n'interdit de s'en approcher, la navigation était libre dans les eaux internationales.

D'après le même journal, la coupure d'un de ces câbles rendrait les liaisons intercontinentales quasiment impossibles dans les fait tant les ressources sont très utilisées avec des possibilité de re-routage très limité dans les faits.

Ultra-rapides puisqu'ils évitent la perte de temps induite par la durée nécessaire pour effectuer une transmission par satellite mais pourtant vulnérables, ces câbles se retrouvent parfois à 1 ou 3 mètres sous le fond à proximité des côtés et au large, touchent le fond des océans. Pas suffisant hélas aujourd'hui pour se mettre à l'abri des menaces humaines et naturelles : Requins, tremblements de terre, bateaux et pêcheurs véreux coupant parfois des kilomètres de câbles pour les revendre comme en 2007 au Vietnam.

En 2015, c'est une ancre qui fût à l'origine d'une section de câble privant presque toute l'Algérie d'Internet pendant deux semaines. Tout comme en Égypte en 2008 (perte immédiate de 70% de sa capacité de connexion à internet).

Actuellement, 99,8% du trafic internet intercontinental transite via 366 câbles sous-marins soit plus d'un million de kilomètres de câbles à fibre optique parsemant le fond des océans. Une fois en surface, ils sont rattachés à des stations d 'atterrissement. Ces dernières sont d'ailleurs elles aussi assujetties aux menaces. « En cas de conflit militaire, si plusieurs câbles sont sabotés,nous risquons rapidement une saturation de notre accès à Internet» s'inquiète Jean-Luc Vuillemin.

Heureusement, des systèmes de secours existent comme le principe de redondance. 01net l'a vulgarisé parfaitement dans ses lignes il y a quelques années : « Les câbles transatlantiques rejoignent eux la Bretagne et la Normandie. Pour garantir les transmissions sous-marines dans les deux sens, plusieurs sécurités sont prévues. Le câble lui-même comporte deux paires de fibres optiques au lieu d'une. Le doublage suffit pour résoudre les problèmes électroniques, comme la panne d'un multiplexeur ou d'un routeur, la plus courante. Chaque opérateur crée ensuite des redondances du réseau en posant plusieurs câbles distants sur chaque liaison desservie. Celle entre la France et les Etats-Unis se répartit entre sept câbles, directs ou transitant par le Royaume-Uni. »

Enfin, certains ont trouvé une alternative au sabotage physique des câbles, les services de renseignements de certains pays avec leurs mouchards placées eux-aussi au fond de l'eau.

Facebook et Microsoft main dans la main

En mai 2016, Facebook et Microsoft ont annoncé la construction en duo d'un câble sous-marin à fibres optiques, qui traversera l'océan Atlantique pour relier Virginia Beach aux USA jusqu'à Bilbao en Espagne.

Le général Keith B. Alexander, chef du Cyber Command veut un deuxième Internet aux Etats-Unis

Pour certains, la cyberguerre est un sujet de scénario de films de science fiction ; pour d'autres, c'est la réalité de la guerre contemporaine.

Dans un entretien avec plusieurs journalistes, dont rend compte cette semaine le New York Times, le général Alexander propose la création d'un réseau Internet distinct de celui qui existe aujourd'hui, afin de sécuriser le réseau électrique américain, considéré comme le maillon faible de la sécurité des Etats-Unis.

Cette proposition d'une ampleur considérable, financièrement et techniquement, est lancée publiquement par le général en anticipation d'une remise à plat de tous les enjeux stratégiques liés à Internet par la Maison Blanche d'ici à janvier. Elle fait partie d'un exercice classique aux Etats-Unis de lobby public en faveur d'arbitrages budgétaires par chaque branche de l'appareil militaire, mais pas seulement.

Des « bombes logiques » dans le réseau électrique

Le réseau électrique américain actuel utilise les réseaux Internet et se révèle donc particulièrement vulnérable. C'est la thèse développée au début de l'année par Richard A. Clarke, un ancien responsable de la Sécurité de l'administration Clinton, dans un livre coécrit avec Robert K. Knake, intitulé « Cyber War : The Next Threat to National Security and What to do About It » (« Cyber guerre : la prochaine menace à la sécurité nationale et ce qu'il faut faire »).

Clarke affirme que les services américains ont découvert dans le réseau électrique américain des « bombes logiques » chinoises. Une « bombe logique », c'est comme un virus informatique, dormant, qui peut se déclencher à distance et des années plus tard si nécessaire. Ces « bombes » auraient pu être introduites par une faille dans le réseau internet utilisé par les producteurs et distributeurs d'électricité.

Dans son livre, Richard A. Clarke utilise cette découverte pour plaider en faveur d'un réseau internet séparé pour les installations vitales des Etats-Unis (comme le montre le schéma ci-dessus).

En effet, selon lui, la vulnérabilité du Net américain peut potentiellement mettre les Etats-Unis à genoux en peu de temps en cas de cyber-attaque, privant le pays d'électricité, de transports, de services d'urgence, et affaiblissant même sa capacité de défense.

L'ancien conseiller de Bill Clinton se livre même à un exercice de simulation de cyberguerre avec la Chine, avec des étudiants, basé sur un scénario étrangement similaire à un sujet de tension entre Washington et Pékin il y a quelques mois, peu après la sortie du livre.

Il imagine ainsi une crise entre la Chine et le Vietnam sur la souveraineté d'îles riches en hydrocarbures dans la mer de Chine, et un engagement de Washington au côté du Vietnam. Ça ne vous rappelle rien ? C'est ce qui s'est produit l'été dernier, sur le plan diplomatique uniquement…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : « Qui a le savoir, a le pouvoir »: Les câbles sous-marins, le maillon faible de la cyberguerre