CHAMBRE ARBITRALE MARITIME DE PARIS

Gazette de la Chambre

Lettre d'information de la Chambre arbitrale maritime de Paris

Comité éditorial : Philippe Delebecque - Claude Goussot - Jean-Yves Thomas - Michel Leparquier

Editeur : Philippe Delebecque

3 numéros par an **(Janvier - Avril - Septembre)** **Numéro 43 - Printemps 2017**

"Res judicata pro veritate habetur"

Les cyber-menaces contre les navires et les installations portuaires

Francis Baudu

Arbitre maritime

Le GPS (*Global Positioning System*) règne en maître car non seulement la navigation mais également la conduite du navire y sont désormais interconnectées, de même que sont également interconnectés grues, portes d'écluses, terminaux de vrac liquide, silos, convoyeurs de vrac sec, etc.

Mais le signal GPS est extrêmement ténu : de l'ordre de 10^{-28} watt, ce qui peut le rendre aisément inexploitable en cas de signal parasite. Or la Chine a fabriqué massivement des brouilleurs que l'on peut se procurer pour 15$ en Thaïlande par exemple.

Pour les navires, la menace se trouve à deux niveaux :

1) le brouillage (*jamming*) par lequel le navire perd le fil de son information et répondra par une route erratique et une navigation erronée. Notons que, par ailleurs, les tempêtes solaires sont un brouilleur naturel, mais les bords reçoivent des mises en garde avant leur survenance.

2) La mystification (*spoofing*) qui fera envoyer par l'A.I.S (*Automatic Identification System*) des positions et indications de route erronées du navire, qui seront reçues et prises en compte par d'autres navires. On imagine la scène de déroute catastrophique si cela se produisait par exemple dans le rail d'Ouessant.

D'autre part, toute la chaîne logistique est aussi menacée : transports routiers, ferroviaires, aériens, fluviaux.

Le 16 avril 2014, le Ropax "Sewol" fait naufrage au S.O. de la Corée du Sud faisant plus de 300 victimes, par temps clair et calme. Son capitaine sera condamné pour bien d'autres manquements, mais de récents travaux d'experts de l'OTAN, qui appellent encore des vérifications, suspecteraient que la cause du naufrage pourrait être aussi en partie due à un brouillage par la Corée du Nord. Cela ne se serait sans doute pas produit si, comme le recommande l'OMI, une autre méthode de navigation (côtière, estime) avait été suivie en parallèle au GPS. Au large, combien de bords tiennent-ils assidûment leur estime, font-ils des points astronomiques, en recoupement du GPS ?

Le même groupe d'experts de l'OTAN a constaté que les nombreux questionnaires à remplir désormais par les bords pour passer des inspections d'affréteurs, les changements d'eau des ballasts en route, les diverses procédures désormais imposées, rendent les personnels moins ou pas disponibles pour tenir une deuxième méthode de navigation en double du GPS, d'autant que l'extrême facilité d'obtention d'un point GPS fiable pour l'officier de quart, ne l'encourage pas à vérifier sa position à l'aide d'une méthode différente.

Une solution a été évoquée, laquelle consisterait à utiliser des systèmes hyperboliques comme le LORAN E, un perfectionnement du LORAN C dont les USA ont condamné les émetteurs dès 2010. Mais le Congrès a remis la question à l'ordre du jour, en envisageant son utilisation comme appui au GPS, prenant conscience de la dépendance non seulement des navires et avions au GPS, mais aussi de celle de nombre d'institutions-clés dont le fonctionnement repose sur l'horloge GPS.

Au sein de l'OTAN, les recommandations en faveur de la remise en service d'émetteurs LORAN ont été freinées par la crainte que cela ne renforce le lobby britannique qui les fabrique.

L'autre type de danger qui affecte le maritime est la cyber-attaque contre les ports. En effet, le secteur maritime est dorénavant totalement organisé autour de la marétique, ensemble des systèmes d'information et de traitement des données relatif aux activités maritimes et portuaires. Un enjeu énorme si l'on considère que 90 % du commerce de l'Europe est maritime, et que plus des 3/4 des denrées ou objets que nous touchons ou utilisons sont passés par la mer à un certain stade de leur transformation. Tout est maintenant largement automatisé, mais le constat doit être fait que ces systèmes n'intègrent que rarement les problématiques de cyber-sécurité.

Un point faible de la marétique portuaire est la forte interconnexion des systèmes. Conçue pour des gains de productivité, elle laisse le champ libre aux intrus hostiles pour se promener à leur gré dans les systèmes d'information interconnectés à Internet sans raison opérationnelle, comme si le code ISPS n'avait rien à faire dans ce domaine ou avait ignoré les cyber-menaces. De même, des débats ont conclu que si les personnels sont parfaitement rompus à toutes les situations d'attaques terroristes, ils ne le sont pas au piratage ou à l'intrusion dans les systèmes marétiques. ***Suite de l'article page 2.***

Suite de l'article " Les cyber-menaces contre les navires et les installations portuaires".

On relève déjà nombre de cyberattaques : apposition de faux visas de vérification par les douanes sur des conteneurs, ce qui a permis le développement d'un important trafic de drogue, vols de conteneurs pré-identifiés, navires déviés de leur route à leur insu, vol de données sur la position et la route d'un navire ayant permis son attaque par des pirates, intrusion hostile dans les systèmes informatiques d'une plateforme offshore dont la stabilité a été détériorée, lui donnant une gîte dangereuse.

Aucun texte n'existe encore pour traiter ces menaces. Au demeurant, il peut falloir des années pour préparer des textes réglementaires et les faire voter, alors que le danger n'attend pas : il est là !

Dès lors que l'imminence de la menace est établie, il faut agir en bon père de famille et ne pas attendre des textes pour se protéger (les coûts de protection sont toujours d'ailleurs augmentés par les règlements).

Nous avons vu sur quels fronts les cahiers des charges doivent prévoir pour les systèmes informatiques un durcissement, des pare-feux, et une formation des personnels. Nous disposons déjà de "RETEX". Ce sont les architectures de tous les systèmes SCADA (*Supervisory Control And Data Acquisition*) qui doivent être repensées. Le GPS est bien né dans le domaine militaire. Inspirons-nous par exemple des systèmes militaires d'acquisition, traitement et transmission de leurs données tactiques.

Pour revenir aux seuls navires, si les navires-poubelles ont pratiquement disparu de nos côtes, la flotte mondiale ne cesse de croître. En effet, chaque être humain génère une part de transport maritime ! La flotte mondiale croît avec la population. Cette flotte est composée de navires aux systèmes sophistiqués armés par des équipages réduits.

Le premier constat signifie qu'il faut mondialement plus de marins, mais le second que leur nombre diminue par navire. Globalement, il y a un déficit de marins et, en corollaire, un manque d'expérience et de formation. Les navires ont gagné en qualité, les équipages ont régressé, alors que simultanément les tâches liées à l'application de règlements mobilisent de plus en plus les marins contraints à un travail administratif. Situation peu propice à la protection contre des cyberattaques, en particulier pour la tenue de deux méthodes simultanées de navigation.

L'intrusion d'un signal pirate déviant le navire de sa route devrait être perçue sans tarder, avec la reprise en mains immédiate de la conduite du navire. Les marins savent-ils encore faire une droite de hauteur, tenir l'estime ? A noter qu'un capitaine s'expose d'ailleurs à une accusation de négligence en ne se reposant que sur le GPS.

Augmenter le nombre de marins par équipage n'est pas la tendance alors que depuis les accidents de l'"Amoco Cadiz", du "Mega Borg" et d'autres, on a conclu que la plupart étaient causés par des erreurs humaines. Les notations de classe comme BV Aut qui supprime le personnel de quart à la machine s'inscrit dans cette tendance à réduire l'intervention humaine. Dès les années 60, des projets virent le jour de navires téléguidés par un navire-mère, le seul avec un équipage. Aujourd'hui, des expérimentations sont conduites pour mettre au point le navire sans équipage. Nous ne reviendrons pas en arrière.

Même sans équipage, deux systèmes de navigation parallèles restent la clef. Certes, il faut renforcer les systèmes GPS aux brouillages et mystifications, si on le peut, mais le second système, par exemple une centrale à inertie doit être indépendant de recalages périodiques de la dérive de ses gyroscopes par GNSS (*Global Navigation Satellite Sytem*), ce qui nous ramène au problème précédent. A l'approche des côtes, en l'absence de GPS différentiel, ce recalage peut être effectué visuellement (relèvement d'amers) ou au radar mais, au large, il doit se faire par point d'étoiles comme savent le faire de façon automatique les périscopes de sous-marins.

La solution pour la protection de la marétique, à la mer ou dans les ports, est une urgence devant l'imminence d'une menace multiforme aux conséquences potentiellement catastrophiques.