Les enjeux informationnels dans le secteur du transport ferroviaire, routier et maritime

EGE Ecole de Guerre Economique

Alexandre CANELLA
Maeva DELAUNAY
Hugo MATKOWSKI
Nicolas RAGOT
Benjamin ROMAN
Noufelé TATOU
Julien VACHEL

Table des matières

Introduction 1
Partie I : Les acteurs du transport en France 2
A. Les acteurs du transport ferroviaire 2
B. Les acteurs du transport routier 6
C. Les acteurs du transport maritime 9
Partie II : Identification des risques informationnels dans le transport 12
A. Confidentialité 12
1. Définition de la confidentialité 12
2. La propriété intellectuelle 14
3. Les attaques à visée réputationnelle 15
4. Le RGPD 16
B. Intégrité 17
1. Qu'est-ce que l'intégrité des données ? 17
2. Les types d'intégrité des données 17
a. L'intégrité physique 17
b. L'intégrité logique 17
3. Les risques relatifs à l'intégrité des données 18
C. Risques informationnels dans le secteur des transports 19
1. Le domaine des transports maritimes 19
2. Le domaine des transports routiers 20
3. Le domaine des transports ferroviaires 22
D. Disponibilité 24
1. La digitalisation du secteur du transport 24
2. La digitalisation, vectrice de vulnérabilités pour le transport ? 26
3. L'internet des objets 27
Partie III Etude de cas 30
A. La protection des données, nouvel enjeu du secteur des transports 30
B. La blockchain comme réponse aux problématiques de protection des données 33
1. Un système sécurisé 33
2. Un système efficace 34
C. La démocratisation de l'outil dans le secteur des transports 34
1. Un (trop) long processus de transport 35
2. La blockchain permet-elle vraiment de créer un climat de confiance ? 37
D. L'apparition de nouvelles problématiques 39
Conclusion 40
ANNEXES 41
COMPTE-RENDUS D'ENTRETIENS 55
SOURCES 62

Introduction

La logistique représente 10 % du PIB national français, 1,8 million d'emplois et un chiffre d'affaires de 200 milliards d'euros pour l'année 2019. Les modes de transports utilisés sont à 87 % du transport routier en interne, 10,6 % de ferroviaire et 2,3 % de fluvial. Elle représente 12 % du chiffre d'affaires des entreprises, tous secteurs confondus selon le ministère de la transition écologique et solidaire.[1]

Ce dernier souligne également le système complexe que représente la logistique, la concurrence importante sur ce secteur et les enjeux du développement numérique de l'ensemble de la filière.

Le transport et la logistique sont des secteurs d'activité d'importance vitale (SAIV) selon un arrêté du 2 juin 2006.[2] Ce secteur fonctionne en complémentarité des autres, puisqu'aucun des autres SAIV ne peut fonctionner sans logistique, qu'elle soit pour des marchandises ou pour du transport de personnes.

C'est cette importance critique qui en fait un secteur de choix pour les attaques informationnelles. La cybersécurité n'étant pas la priorité pour les entreprises de ce secteur générant peu de rentabilité du fait des charges importantes pour celles-ci (maintien des entrepôts et du matériel de transport, normes de sécurité élevées pour les transports publics, etc.), les attaques informatiques se multiplient. Les dégâts sont également très importants : si la supply chain s'arrête ou si les transports publics sont inutilisables, tous les autres secteurs sont également impactés négativement.

Il convient alors de s'interroger sur les risques informationnels liés au secteur de la logistique, en identifiant d'abord les acteurs français, puis en décrivant les trois principaux risques encourus (confidentialité, intégrité, disponibilité). Enfin, une étude de cas sur la blockchain et ses enjeux dans le transport maritime permettra d'illustrer la prise en compte de ces risques pour assurer une chaîne logistique efficace et plus sécurisée.

Ce dossier traite du transport de marchandises et de voyageurs, dans les secteurs ferroviaires, routiers et maritimes. Il a pour but de dresser un bilan des risques informationnels, et plus particulièrement informatiques, de ce secteur.

[1] « France Logistique 2025 », Ministère de la Transition écologique et solidaire, 29/09/2019.

[2] «Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdit secteurs », Legifrance.

Partie I : Les acteurs du transport en France

Avant d'aborder les risques du secteur du transport, il faut en connaître les acteurs. C'est pourquoi nous décrirons ici les acteurs du transport ferroviaire, routier puis maritime.

A. Les acteurs du transport ferroviaire

Pour consulter la cartographie des acteurs, se reporter à **l'annexe 1**.

Dans le secteur du transport, le secteur ferroviaire est représenté au travers un réseau d'infrastructures implanté sur l'ensemble du territoire avec un point de convergence à Paris, couvrant les grandes villes et les frontières avec les pays limitrophes (cf. Figure 1 : Couverture nationale du réseau ferré en France). Il est considéré comme le deuxième réseau ferré européen et le onzième au rang mondial en 2018 avec 28 000 kilomètres de rails[3]. Ce classement est notamment dû à la prédominance du transport de voyageurs grâce aux lignes à grande vitesse, face au fret, dont l'activité décroit (« 10 % du secteur du transport intérieur terrestre de marchandises »[4]).

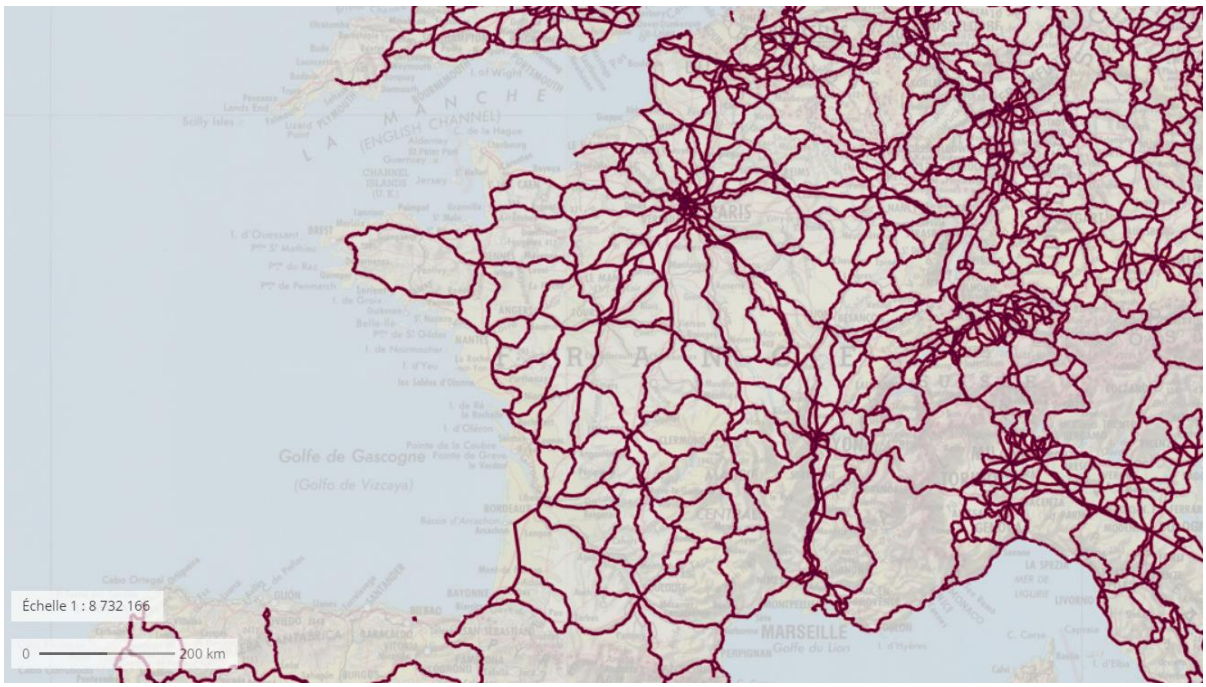


Figure 1 : Couverture nationale du réseau ferré en France (Source : geoportail.gouv.fr - 2020)

Pour satisfaire la demande, des entreprises implantées sur le territoire français permettent d'approvisionner le secteur aux différents stades de la chaine de production et d'utiliser le réseau ferré, au travers des activités suivantes :

[3] « *Le transport ferroviaire en France – Faits et chiffres* », Statista Research Department, 17/03/2020.

[4] « *Transport ferroviaire de marchandises* », Ministère de la Transition écologique et solidaire, 12/11/2018.

- Conception, construction d'infrastructures ferroviaires ;
- Production de véhicules sur rail ;
- Fret ferroviaire ;
- Transport de voyageurs ;
- Maintenance des réseaux routiers et des véhicules sur rail ;
- Sécurité des chantiers et des réseaux ferroviaires.[5]

Elles sont réparties majoritairement dans les régions où le réseau est le plus représenté (cf. Figure 2 : Répartition des entreprises du secteur ferroviaire sur le territoire français).

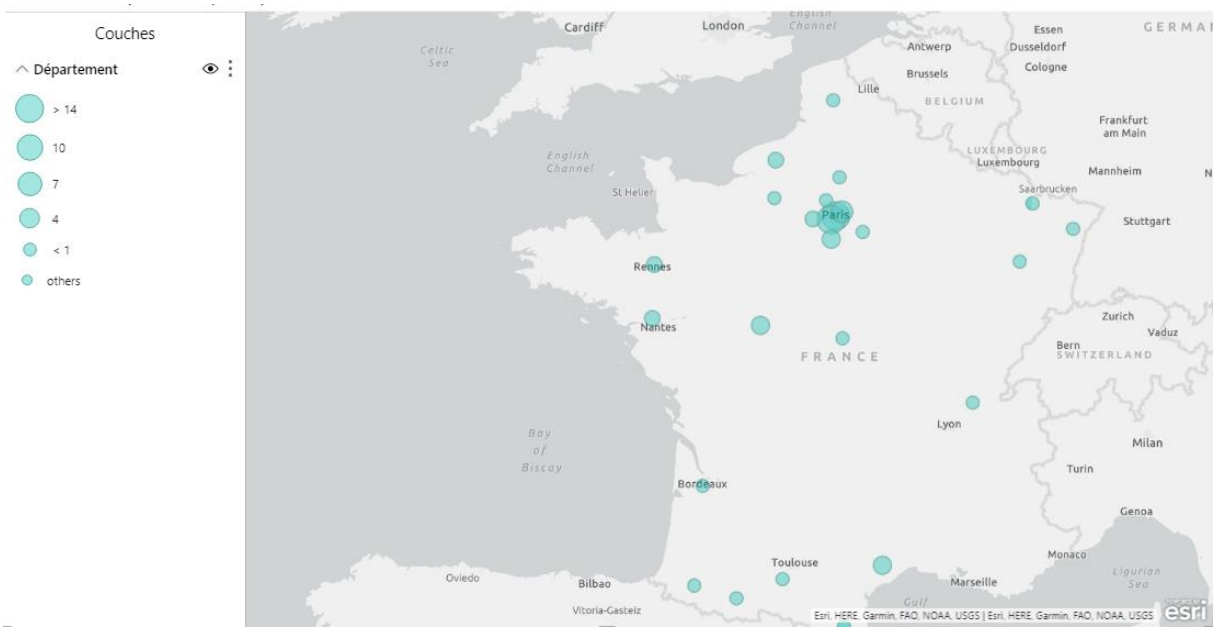


Figure 2 : Répartition des entreprises du secteur ferroviaire sur le territoire français (Source : RSIC02 – ESRI- 2020)

En effet, comme l'illustre le graphique ci-dessous (cf. Figure 3 : Nombre d'entreprises du secteur ferroviaire par département français), Paris concentre le plus grand nombre d'entreprises parmi les départements français, en totalisant quinze. Le département des Hauts-de-Seine

[5] Fédération des industries ferroviaires.

s'impose en seconde place avec quatorze entreprises puis, il faut attendre la troisième place pour quitter l'Ile-de-France, avec le département Nord.

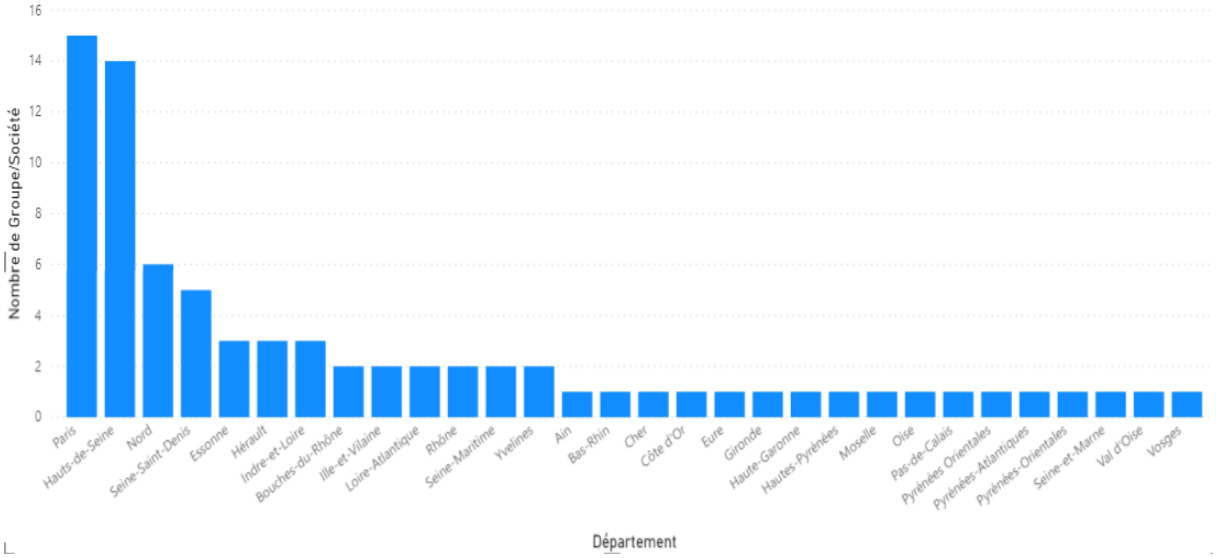


Figure 3 : Nombre d'entreprises du secteur ferroviaire par département français (Source : RSIC02 – ESRI - 2020)

Concernant l'exploitation du réseau ferré national, le quasi-monopole du secteur est attribué à la Société Nationale des Chemins de Fer français (SNCF), qui appartient à l'Etat.

Cependant, grâce à l'ensemble des entreprises publiques et privées du secteur, les véhicules ferrés de la flotte au rang national constituent les TGV, les RER (Ile-de-France), les TER, les métros (Lille, Lyon, Marseille, Paris, Rennes et Toulouse), les tramways (28 communes).

Contrastant avec cette activité, le transport de voyageurs et le fret ouvrent le marché aux entreprises du secteur privé, y compris des entreprises étrangères.

De ce fait, bien que de grands groupes français intègrent des filiales dans ce secteur, comme la SNCF, Eiffage TransDev, ou encore VINCI, la France est loin d'être autarcique dans ce secteur. Des entreprises, dont le siège social se situe en France, sont en réalité absorbées par des groupes étrangers, provenant majoritairement de pays limitrophes de la France. L'Amérique du Nord est également concernée, tant les Etats-Unis que le Canada (cf. Figure 4 : Localisation des Groupes étrangers du secteur ferroviaire présents en France).

La Chine, quant à elle, commence à s'intéresser au savoir-faire français dans la fabrication de matériel ferroviaire. Cela lui est permis grâce, notamment, au Groupe MA STEEL, qui a repris dans le Nord de la France, l'entreprise VALDUNES, fabricant de matériel roulant ferroviaire, alors en redressement judiciaire[6] (cf. **Annexe 2 :** Article de Usine Nouvelle sur la reprise de Valdunes par MA Steel.).

[6] Francis Dudzinski, « *Le chinois MA Steel reprend Valdunes* » Usinenouvelle.com, 02/06/2014.

Figure 4 : Localisation des Groupes étrangers du secteur ferroviaire présents en France (Source : RSIC02 – ESRI - 2020)

Le graphique ci-dessous (cf. Figure 5 : Nombre de Groupes du secteur ferroviaire présents en France par pays), représente l'Espagne, l'Allemagne et la Belgique comme les pays les plus impliqués dans le secteur ferroviaire français, au travers de groupes économiques qui possèdent des filiales dans ce pays. Toujours sur ce critère, les pays d'Asie et d'Amérique du Nord précités se placent après les pays d'Europe de l'Ouest, sauf le Luxembourg, qui arrive en neuvième place.

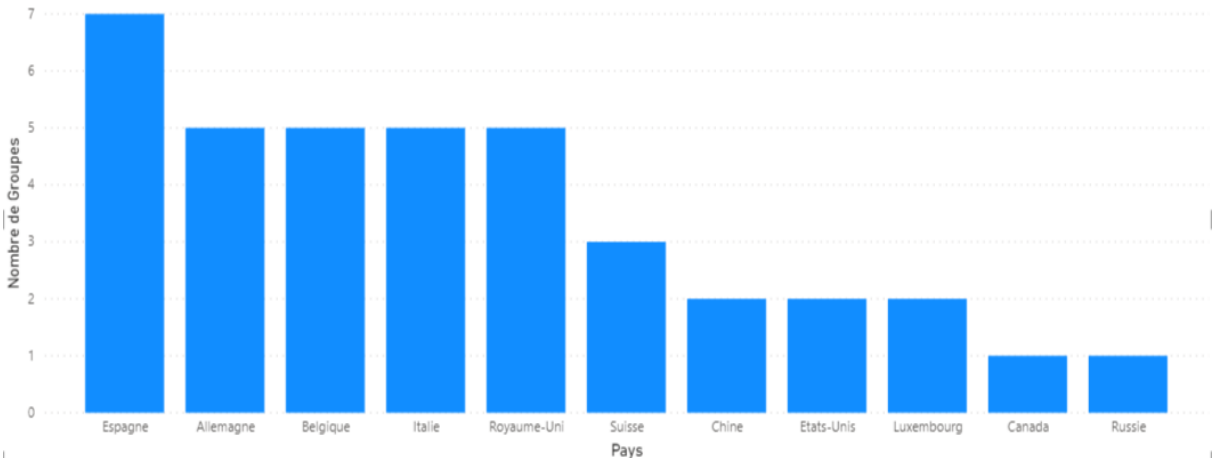


Figure 5 : Nombre de Groupes du secteur ferroviaire présents en France par pays (Source : RSIC02 - ESRI - 2020)

Dans la globalité, les organisations étrangères s'intéressent aux constructeurs ferroviaires mais plus particulièrement aux transporteurs de marchandises et de voyageurs. C'est le cas, notamment, des groupes présents dans les pays limitrophes. L'espace SCHENGEN, zone de libre-échange des personnes et des biens, est le témoin d'une coopération étatique. De ce fait, des groupes français et étrangers peuvent se partager plus facilement les actions d'une même entreprise basée en France.

A l'heure actuelle, les entreprises et les groupes spécialisés dans le transport ferroviaire sur le territoire français sont majoritairement représentés en Ile-de-France, dans les Hauts-de-France et le Sud du pays. Cependant la cartographie (cf. **Annexe 1** : Cartographie des organisations du secteur ferroviaire présentes en France) démontre la difficulté de la France à être souveraine dans ce secteur, notamment lorsque les organisations étrangères interviennent dans la production des infrastructures et des véhicules ferroviaires. Cependant, cette internationalisation permet aussi au secteur de se développer à l'étranger en exportant son savoir-faire dans les pays concernés et d'exporter le réseau à la française. Malgré les intérêts financiers potentiels liés à cette externalisation nationale et ces coopérations étrangères, le risque informationnel du secteur ferroviaire est à prendre en compte.

B. Les acteurs du transport routier

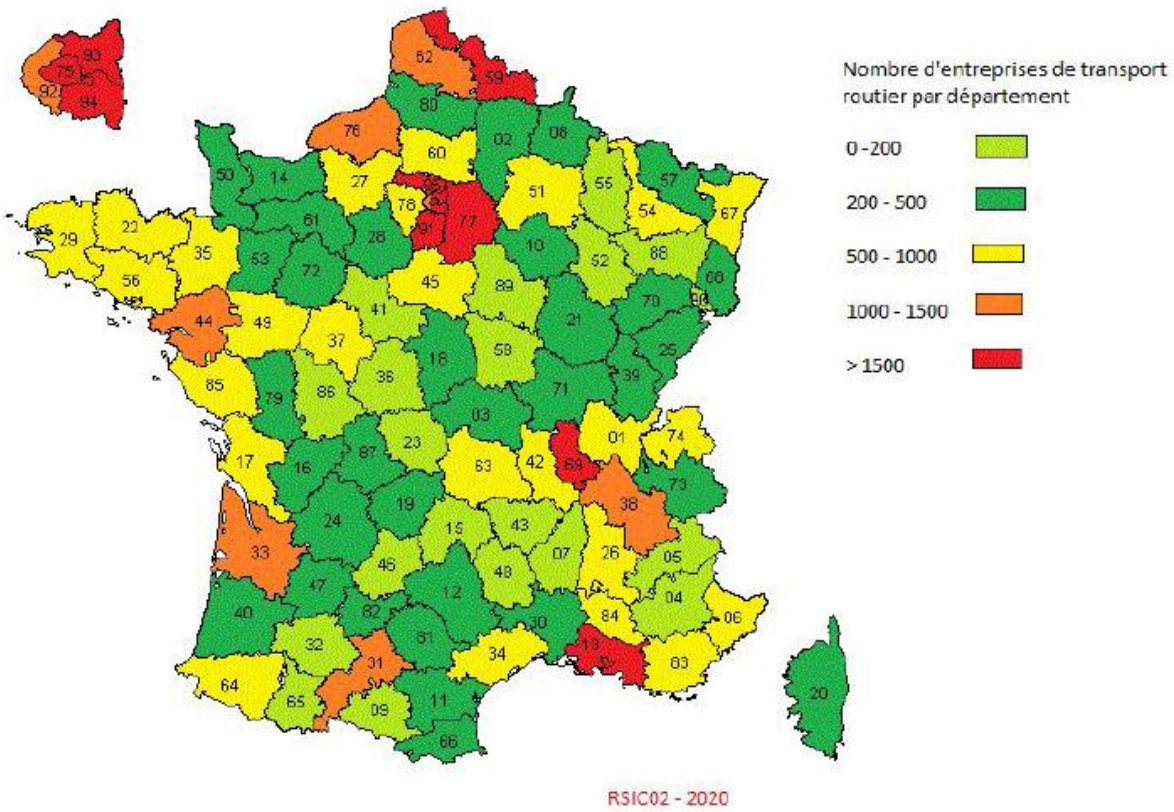


Figure 6 : Nombre d'entreprises de transport routier par département (Source : RSIC02 - 2020)[7]

Les données exactes utilisées pour cette cartographie sont répertoriées dans **l'annexe 3** « cartographie transport ».

[7] *Liste des entreprises de transport de marchandises par département,* Chauffeur Poids Lourd, 2018 ;

Les chiffres présentés par cette carte (cf. Figure 6 : Nombre d'entreprises de transport routier par département) permettent d'apprécier la répartition des entreprises de transport routier sur la totalité du territoire national. Cette absence de concentration de l'activité couplée au nombre important d'entreprises implantées sur notre territoire rend la protection du secteur particulièrement difficile. Il semble plus pratique de décentraliser le soutien de l'Etat français car une démocratisation de l'intelligence territoriale pourrait profiter à ces entreprises en les aidant à pérenniser leurs activités. Il est cependant important de noter la forte concentration d'entreprises de transport en Île-de-France, dans les départements 13 et 69, ainsi que dans certains départements portuaires ou proches des frontières.

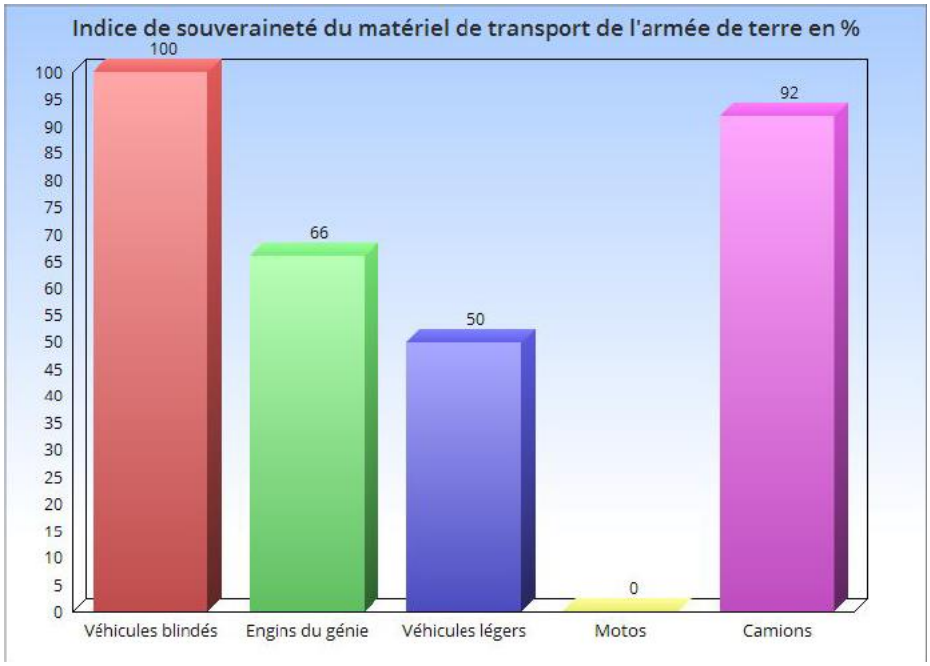
Les grands groupes sont certainement plus exposés que les Petites et Moyennes Entreprises (PME), mais aussi mieux préparés et plus prudents. Les efforts de l'État doivent se concentrer sur ces puissants acteurs, mais les régions et départements se doivent d'allouer des moyens pour protéger ce secteur. Les acteurs locaux sont plus à même de cerner les opportunités et menaces de ces petites entreprises qui n'évoluent pas sur le même échiquier que les grands groupes, et, par extension, de fournir des solutions plus adaptées.

De plus, les entreprises françaises de transport doivent œuvrer aux côtés d'autres acteurs nationaux afin de tisser un réseau de moins en moins perméable aux attaques informationnelles, servant tant les petites entreprises que les champions nationaux.

Les entreprises telles que Chronopost ont recours à la sous-traitance afin d'assurer la continuité de leurs services et s'exposent de ce fait à des attaques informationnelles potentielles[8]. De cette interconnexion entre nos sociétés de transport ressort la nécessité de protéger chacun des acteurs pour le bien commun du secteur du transport routier, protection qui doit être opérée tant au niveau national que territorial.

[8] Source humaine, sous-traitant de Chronopost dans le département 74 ;

- Focus sur le transport des véhicules militaires



9 10 11 12 13 14 15 16 17 18

Figure 7 : Indice de souveraineté du matériel de transport de l'armée de terre en % (Source : RSIC02 - 2020)

L'indice de souveraineté exprime le pourcentage de véhicules produits par la France. Il comporte des approximations et des inconnues, symbolisées par « * » dans la cartographie du transport routier (cf. **Annexe 3** : Cartographie des organisations du secteur routier présentes en France). Au sein même de l'armée, l'un des piliers étatiques, il semble contradictoire d'observer une présence aussi importante de matériel étranger. Ne serait-il pas souhaitable de contrôler la totalité de la chaîne de production et d'approvisionnement de notre matériel militaire ? La mondialisation rend cette tâche quasiment impossible, mais il serait malhonnête de ne pas le souligner. L'éclatement des chaînes de production, la multiplicité des sous-traitants et une interconnexion planétaire accroissent drastiquement le risque de fuites informationnelles. Il est cependant nécessaire de diminuer au maximum ce risque tant pour l'armée que pour le civil, en

[9] Laurent Lagneau, « Le parc de véhicules P4 de l'armée de Terre fond à vue d'œil », Opex 360, 03/03/2013.

[10] « Defender : le véhicule polyvalent de l'armée de Terre », Ministère des Armées, 28/06/2010.

[11] D. L., « Quand l'armée française préfère rouler américain », BFM Business, 04/05/2015.

[12] Laurent Lagneau, « Le ministère de la Défense a commandé 520 véhicules pour l'opération Sentinelle », Opex 360, 10/02/2016.

[13] Laurent Lagneau, « L'armée de Terre a reçu 150 motos Yamaha XTZ 660 Ténéré », Opex 360, 17/04/2015.

[14] « Les chiffres clés de la Défense 2019 », Ministère des Armées, 28/08/2019.

[15] « Les chiffres clés de la Défense 2018 », Ministère des Armées, 11/09/2018.

[16] Laurent Lagneau, « Nexter a livré le dernier Engin Blindé du Génie-VALorisé à l'armée de Terre », Opex 360, 05/02/2014.

[17]« PTA 2 » Military Today.

[18] « Véhicules », Ministère des Armées.

privilégiant le matériel français ou, à minima, des partenaires européens si les caractéristiques de ce matériel restent compétitives. Afin de mieux contrôler le risque informationnel, il est nécessaire de posséder une certaine emprise sur sa chaîne de production et d'approvisionnement. Il est particulièrement inquiétant de voir l'armée équipée de matériel extra européen, surtout en provenance des États-Unis, connus pour leurs techniques agressives en matière d'espionnage. Il en va de même pour les Five Eyes (Australie, Canada, Nouvelle-Zélande, Royaume-Uni), alliés des États-Unis.

Une rupture des échanges commerciaux entre la France et ses partenaires en raison d'une crise spontanée est très peu probable. Cependant, ce scénario pourrait se révéler dramatique pour notre État et porter atteinte à notre capacité de défense en cas de conflit armé. Nous avons pu observer au cours de la crise du coronavirus que l'intérêt national prime sur les intérêts des partenaires économiques. La relocalisation de notre industrie automobile couplée à une préférence pour le matériel français pourrait grandement aider l'armée à se prémunir de certaines attaques informationnelles.

C. Les acteurs du transport maritime

Pour consulter la cartographie des acteurs, se reporter à l'**annexe 4**.

Le secteur du transport maritime et fluvial représentait, en 2019, un budget d'environ 32 milliards d'euros. Forte de son réseau navigable de plus de 4770 km et de ses onze Grands Ports Maritimes (GPM), étendant son influence au monde entier, la France est une puissance incontestable de ce secteur qui agglomère 80 % du volume et 70 % de la valeur des marchandises échangées dans le monde en 2015. Une puissance dont le représentant majeur CMA-CGM est le quatrième armateur le plus important au monde derrière Maersk, MSC et COSCO group.[19]

Le transport maritime assure aujourd'hui 78 % des importations françaises et génère un chiffre d'affaires de près de 690 millions d'euros pour les GPM. En outre, ce sont près de 32 millions de passagers qui transitent sur les lignes internationales et les croisières. Il est évident que le secteur du transport maritime revêt une importance stratégique pour la France[20].

Les recherches conduites sur l'écosystème du transport maritime en France ont produit des résultats parlants. La cartographie (cf. **Annexe 4 :** Cartographie des organisations du secteur maritime présentes en France) montre que la flotte militaire française est largement indépendante des réseaux et constructeurs étrangers. En effet, cinq entreprises (Naval Group, Chantiers de l'Atlantique, CMN, Socarenam et CNIM) ont fourni la quasi-totalité de cette flotte. À cette règle, trois exceptions existent :

[19] « Les chiffres du transport fluvial et maritime 2019 » *Clic & Sea,* 2019.

[20] « La France acteur maritime du 21e siècle », *Direction des affaires maritimes,* 2019.

- Le MN Calao et le MN Tangara issus du chantier naval Hyundai Mipo Dockyard. Ces deux navires sont des navires marchands sous pavillon français de la compagnie maritime nantaise et affrétés à temps plein pour les besoins des armées françaises.
- Le Dupuy-de-Lôme, navire collecteur de renseignements de la marine française travaillant au profit de la Direction du Renseignement Militaire (DRM). Ce bâtiment, bien que dessiné par les soins de Thalès, a été fabriqué et vendu par la Royal Niestern Sander, compagnie hollandaise.[21]

Il serait probablement plus judicieux d'employer un navire de construction française pour remplir la fonction du Dupuy-de-Lôme. En effet, à sa livraison, celui-ci possède ce qui se fait de mieux en termes de technologies de l'information. L'électronique y est donc omniprésente. C'est pourquoi le choix d'un prestataire étranger pose question, notamment quand des chantiers navals français auraient été qualifiés pour répondre à cette commande. Cependant, le navire en question est en service depuis 2005 et aucun problème n'a été révélé publiquement depuis lors.

On peut donc affirmer que de ce point de vue, la France est bien sensibilisée au risque informationnel qui pèse sur ses navires militaires, qui jouent un rôle crucial dans le statut de puissance navale attribué à notre pays.

De plus, il est important de noter que les principaux fournisseurs de navires de recherche sont français. Il s'agit de Naval Group et des Ateliers et Chantiers du Havre.

En revanche, en ce qui concerne les navires câbliers, de transport de marchandises ainsi que de personnes, la donne n'est plus la même. La cartographie (cf. **Annexe 4 :** Cartographie des organisations du secteur maritime présentes en France) permet de visualiser la dépendance française vis-à-vis des constructeurs et fournisseurs étrangers dans ces industries. D'une part, les câbliers français sont d'origine roumaine ou coréenne. D'autre part, le fleuron de la marine marchande hexagonale qu'est CMA-CGM, est fourni en porte-conteneurs et vraquiers par les géants coréens et chinois Samsung, Hyundai, DSME et CSSC. Enfin, le navire amiral de l'entreprise, le CMA-CGM Antoine de Saint Exupéry est de fabrication Philippine, par l'entreprise Hanjin Heavy Industries and Construction.[22]

Pour être plus pertinent, seuls les principaux fournisseurs ont été mentionnés dans la cartographie, mais l'essentiel des bâtiments possédés par CMA-CGM sont issus de l'étranger. Ce qui pose un réel problème de dépendance, notamment vis-à-vis des entreprises coréennes, c'est que les liens avec leur gouvernement sont solides bien qu'officieux.

En ce qui concerne le transport de personnes, les Chantiers de l'Atlantique représentent le chantier naval français le plus important avec un chiffre d'affaires de plus d'1.8 milliard d'euros

[21] « Liste des navires de la Marine nationale (France) », *Wikipedia.*

[22] « Flotte », CMA-CGM.

en 2018. Ce chiffre représente l'ensemble de l'activité mais pas uniquement le transport de personnes. Cependant, ce marché est très concurrentiel et nombre d'entreprises étrangères sont solidement implantées sur le territoire. Les entreprises françaises, plus modestes ont donc du mal à trouver leur place dans ce marché dominé par des géants de l'industrie tels que le britannique P&O, l'italien Grimaldi ou encore le suédois Stena concernant les navires rapides comme les ferries[23], et la Royal Caribbean Cruise Line (24 % de parts de marché), Norwegian Cruise Line (9 %) et MSC Croisières (7 %) pour ce qui est des croisières[24].

[23] « Le transport de passagers : ferries et navires rapides », Armateurs de France.

[24] Vincent CALABRESE, « La croisière, un marché qui continue de croître », L'antenne, 26/09/2018.

Partie II : Identification des risques informationnels dans le transport

Cette multitude d'acteurs — depuis leur entrée dans une économie digitalisée et mondialisée — est en proie aux risques informationnels, caractérisés par le niveau de besoin de sécurité de l'information, formalisé sous trois critères : la confidentialité, l'intégrité et la disponibilité de l'information.

A. Confidentialité

1. Définition de la confidentialité

Face à la guerre économique à laquelle sont confrontées les entreprises françaises, la dimension de la confidentialité des données[25] est un atout majeur dans leur compétitivité : la guerre par l'information les frappe de plein fouet. Avant de parler de confidentialité des données, il s'agit d'évaluer les informations et de les hiérarchiser, de l'information publique à l'information vitale, confidentielle : « droit d'en connaître (least privilege) ». L'enjeu est de préserver le patrimoine informationnel de l'entreprise.

Assurer son patrimoine informationnel, c'est d'abord analyser et traiter l'information. Pour cela, il est possible de classer les informations selon le cycle suivant[26] :

- Première étape : **Identifier** l'information et son propriétaire ;
- Deuxième étape : **Connaître** et **maitriser** son cycle de vie ;
- Troisième étape : **Hiérarchiser** l'information selon son niveau de sensibilité ;
- Quatrième étape : **Évaluer** les impacts de la perte d'information. **Évaluer** les risques pour l'entreprise ;
- Cinquième étape : **Identifier** les mesures de sécurité à mettre en place et **veiller** à l'application stricte des mesures ;
- Sixième étape : **Maintenir** le dispositif opérationnel.

Cette logique doit permettre à l'entreprise de répondre à plusieurs questions, notamment aux suivantes : Comment établir qu'une information est critique ? Comment communiquer cette information ? Qui doit être le destinataire ? Ces questions relèvent du domaine de l'intelligence économique. La protection des actifs informationnels permet donc à l'entreprise d'asseoir sa compétitivité. Il est en effet illusoire de vouloir protéger l'ensemble de ces informations sans définir au préalable un degré de sensibilité (voir tableau ci-après).

[25] A. Fandi « Cybersécurité et culture d'entreprise », Les Echos, 13/11/2019.

[26] « La classification au sein de l'entreprise : Enjeux et Démarche pragmatique », LMPS groupe, 2016.

A titre d'exemple, les informations stratégiques communes à une majorité d'entreprise, sont les données RH, les applications de comptabilité, les contrats, etc.

Dans l'objectif de préserver ces actifs informationnels, il apparaît nécessaire d'établir une échelle de classification de l'information, en particulier sur le volet de la confidentialité.

Le tableau suivant présente un modèle permettant d'évaluer le degré de sensibilité de l'information.

Confidentialité	Description de l'expression du besoin	Niveau de l'impact redouté
Confidentiel	L'information est critique. En cas de fuite, les impacts sont maximums. Les destinataires et propriétaires sont peu nombreux. Les moyens de communication sont chiffrés et seuls les propriétaires et destinataires connaissent la clé.	C4
Réservé	L'information est stratégique. En cas de fuite, les impacts sont importants. Les destinataires et propriétaires sont peu nombreux. Un mot de passe peut être demandé.	C3
Limité/interne	L'information a vocation à rester en interne. Elle est nécessaire aux activités de l'entreprise. La communication par mail est autorisée. Peu d'impact en cas de fuite de données.	C2
Public	L'information n'a pas de valeur interne, elle peut être rendue publique sans impact pour l'entreprise.	C1

Tableau 1 : Degré de sensibilité de l'information (confidentialité)

Pour les entreprises les plus résilientes et où la concurrence est rude (comme le secteur des transports par exemple), il est conseillé de capitaliser sur la sécurité de l'information. Cela peut se traduire par la construction d'une fiche de sécurité de l'information.

Fiche de sécurité de l'information

Nom de l'information : Doit être explicite et permettre de la catégoriser (secteurs, business unit, etc.). La date de création et potentiellement la date d'expiration doivent y figurer ;

Propriétaire de l'information : responsable de la gestion de l'information et la personne l'ayant produite. Gestion des droits d'accès (lecture, modification, effacement) ;

Format de l'information : oral, écrit (mail, papier) ;

Impact de l'information sur l'entreprise : opérationnel, financier, conformité, etc. ;

Besoins de sécurité : degré de confidentialité (C0, [...], C4) ;

Canal de diffusion : dépendant du degré de confidentialité (mail, sms, appel téléphonique, etc.) ;

Support de stockage : base de données, applications, serveurs, disques durs, etc. ;

Procédure de destruction de l'information : mise à jour, effacement.

Les mesures de sécurité : règles d'authentification, chiffrement.

En réalisant ce travail, l'entreprise a une vision claire des enjeux stratégiques de son patrimoine informationnel. Elle peut, dès lors, maîtriser et contrôler l'information[27], ce qui présente deux avantages majeurs : d'une part, elle augmente sa compétitivité (volet défensif et offensif) et d'autre part, en cas de fuite ou vol de l'information, il est plus aisé d'identifier l'origine de la faille.

Exemple d'une entreprise ayant subi une cyberattaque altérant la confidentialité de ses données

En juin 2017, la société de transport Maersk, spécialiste dans les navires et les porte-conteneurs, est victime de la cyberattaque mondiale Petya. Le ransomware a chiffré les données de la société, entrainant une perte nette de trois cents millions de dollars. Elle a dû également réinstaller quatre mille serveurs, quarante-cinq mille PC et vingt-cinq mille applications.[28]

Mais la confidentialité des données n'est pas uniquement affectée par des attaques informatiques.

2. La propriété intellectuelle

Le transport est un secteur où de nombreux acteurs se font concurrence. La compétitivité d'une entreprise repose notamment sur la technologie qu'elle utilise et sur sa liste de clients.

[27] A, Juillet : « *L'intelligence économique, c'est l'art de protéger et de maîtriser les informations stratégiques utiles aux acteurs économiques* ».

[28] D, Palmer. « Ransomware : la principale leçon de Maersk dans son combat contre NotPetya », ZDNET, 03 /03/2020.

Afin d'obtenir une technologie adéquate et une liste de clients permettant d'être rentables, des investissements financiers sont indispensables.

Pour développer un système de livraison par drones par exemple, une entreprise doit consacrer une part importante de son budget en Recherche et Développement (R&D) afin de s'assurer de la faisabilité d'un tel projet, mais également effectuer une étude de marché afin d'identifier les potentiels clients. C'est d'ailleurs le cas d'Amazon et de la Poste[29] qui cherchent actuellement à développer ce type d'offre sur le territoire français notamment.

Si un concurrent obtient le résultat de ces recherches sans effectuer des dépenses similaires, l'entreprise devient beaucoup plus compétitive.

Afin de limiter ce risque, l'ensemble des informations doivent être classifiées afin d'identifier celles dites « stratégiques / sensibles ». Les échanges concernant les documents les plus confidentiels doivent ainsi être restreints, limitant in fine les risques qu'ils soient divulgués.

En tout état de cause, les travaux liés à la R&D doivent faire l'objet d'une attention particulière et les innovations en découlant doivent être protégées, notamment par le biais de brevets.

L'industrie de l'automobile est particulièrement active à ce niveau et représentait par exemple, en 2018, 32,8 % des demandes de brevets publiées à l'Institut National de la Propriété Industrielle (INPI)[30].

3. Les attaques à visée réputationnelle

Des attaques à visées réputationnelles peuvent émaner aussi bien de concurrents directs que d'acteurs de la société civile.

Il peut s'agir de critiques concernant les conditions de travail des collaborateurs, le respect des obligations légales ou encore l'adéquation des engagements environnementaux annoncés avec ceux réellement mis en place.

Selon le type d'attaque, la défense de l'entreprise peut être individuelle par le biais d'un communiqué ou collective si un même type de transport est ciblé.

Concernant le secteur de transport, le respect des limites horaires de travail, l'adéquation des mesures de protection octroyées aux salariés avec les risques auxquels ils sont exposés, ainsi que la limitation de son impact environnemental, apparaissent primordiaux. Le dieselgate[31] et plus

[29] Christophe Alix, « *Livraison par drones : Amazon ouvre un centre de R&D à Clichy-la-Garenne* », Libération, 18/05/2017.

[30] Emmanuelle Fortune, Mickaël Chion, « *Focus déposants de brevets à l'INPI en 2018* », Observatoire de la propriété intellectuelle de l'INPI , Décembre 2019.

[31] L'Expansion l'Express, « *Le Dieselgate, scandale automobile de triche généralisée aux contrôles pollution* ».

récemment l'évolution du contexte sanitaire[32] lié au COVID-19 ont démontré que l'activité peut être impactée significativement en cas de non-respect de ces obligations.

Quoi qu'il en soit, à l'heure de la transparence, l'exemplarité des entreprises permet de limiter la portée et la gravité des attaques à visée réputationnelle.

4. Le RGPD

Face au Règlement Général sur la Protection des Données (RGPD), les entreprises ont une obligation légale d'assurer la sécurité des données personnelles dont elles disposent.

En cas de non-respect, celles-ci s'exposent à des sanctions pécuniaires (dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial[33]), mais aussi et surtout les différentes parties prenantes risquent de ne plus vouloir traiter avec l'entreprise concernée.

Si un collaborateur, ou un individu externe à l'entreprise divulgue, volontairement ou non, de telles informations, les conséquences tant pécuniaires que réputationnelles seront donc importantes. Afin de limiter ce risque, les entreprises doivent s'efforcer de limiter l'accès à ces données et les supprimer dès lors que leur usage n'est plus requis.

En outre, toute collecte de données doit être justifiée et limitée au but poursuivi. Ainsi, une entreprise spécialisée dans la livraison terrestre pourra décider de recourir à un système de tracking comme le Global Positioning System (GPS), si cela est nécessaire à la sécurité des personnes ou des marchandises transportées, ou encore au suivi du temps de travail des employés, lorsque ce suivi ne peut être réalisé par d'autres moyens.

En revanche, la collecte des données de localisation est proscrite dès lors que le collaborateur dispose d'une liberté de déplacements, ou dans le cas où le véhicule est utilisé sur son temps de repos[34].

En tout état de cause, dès lors qu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, une Analyse d'Impact Relative à la Protection des Données (AIPD)[35] doit être effectuée.

---

[32] Nolwenn Cosson et Adeline Daboval, « *Fermeture des entrepôts Amazon : les coulisses d'une décision radicale* », Le Parisien, 15/04/2020.

[33] Site de la Commission nationale de l'informatique et des libertés (CNIL), Sanction.

[34] Site de la Commission nationale de l'informatique et des libertés (CNIL), « *Les dispositifs de géolocalisation GSM/GPS* », 15/06/2009.

[35] Site de la Commission nationale de l'informatique et des libertés (CNIL), « *L'analyse d'impact relative à la protection des données (AIPD)* ».

B. Intégrité

L'intégrité implique la maitrise de la fiabilité des données. Il apparait primordial de vérifier la provenance des données, c'est-à-dire leur authenticité, mais également être sûr qu'elles n'aient pas subi de modifications, que ce soit par erreur ou par malveillance.

1. Qu'est-ce que l'intégrité des données ?

Il s'agit de l'exactitude, l'exhaustivité et la cohérence globale des données, mais aussi leur sûreté concernant la conformité à la réglementation — par exemple la conformité au RGPD et la sécurité.

Pendant la phase de conception, on peut s'assurer de cette intégrité par l'application d'un ensemble de règles, normes et processus. L'intégrité des données sert par ailleurs de « rempart » contre les forces extérieures.

2. Les types d'intégrité des données

On distingue deux types d'intégrité des données : l'intégrité physique et l'intégrité logique, obtenues par un ensemble de processus et méthodes permettant de s'assurer de l'intégrité des données dans les bases de données hiérarchiques et relationnelles.

a. L'intégrité physique

C'est la protection de l'unité (contenant de la donnée : data center, disque dur) et de l'exactitude des données lors de leur stockage et récupération. Cette protection (ou intégrité physique) est menacée, par exemple, lors de catastrophes naturelles, de coupures de courant, ou de piratages des fonctions de la base de données. De même, les erreurs humaines, la détérioration du stockage, entre autres, peuvent empêcher d'obtenir les données précises dont auraient besoin par exemple, les programmeurs système, les vérificateurs internes, etc.

b. L'intégrité logique

C'est celle qui conserve les données inchangées pendant leurs différentes utilisations dans une base de données relationnelle. Tout comme l'intégrité physique, mais d'une autre manière, l'intégrité logique protège par ailleurs les données contre les erreurs humaines et le piratage informatique. Nous allons maintenant développer les quatre types d'intégrité logique que nous pouvons rencontrer.

L'intégrité de l'entité *:* il s'agit de garantir que les données ne soient pas répertoriées plus d'une fois et qu'aucune zone de la table ne soit nulle. On utilise, pour ce faire, des clés primaires, ou des valeurs uniques, identifiant des données.

L'intégrité référentielle *:* Elle désigne la série de processus nécessaires pour garantir un stockage et une utilisation homogènes des données. Par l'intermédiaire de règles intégrées dans la *structure de la base de données concernant l'utilisation des clés étrangères, on s'assure que seuls les changements / ajouts / suppressions de données nécessaires et appropriées sont réalisés (par exemple, contrainte pour éliminer l'entrée de doublons).*

L'intégrité de domaine : *Cela permet de se prémunir contre des attaques typosquatting, c'est-à-dire, s'assurer que le client souhaitant se rendre sur le site web accède bien au domaine officiel.*

L'intégrité définie par l'utilisateur *: L'utilisateur a la possibilité, afin de satisfaire des besoins particuliers, de créer d'autres règles et contraintes qui viennent soutenir les différents types d'intégrité logique cités précédemment. C'est souvent le cas lorsque l'on doit prendre en compte des règles spécifiques d'entreprise.*

3. Les risques relatifs à l'intégrité des données

Comme exemple de facteur pouvant affecter l'intégrité des données stockées, nous pouvons citer :

- L'erreur humaine : saisie incorrecte ou effacement des données, erreurs dans l'application des procédures, etc. ;
- Les erreurs de transfert : par exemple, quand des données ne peuvent pas être transférées correctement d'un emplacement d'une base de données à un autre, ou encore quand la donnée est présente dans la table de destination, mais pas dans la table source ;
- Les bugs et virus : logiciels espions ou malveillants, les virus pouvant altérer, effacer les données ;
- Un matériel compromis : ces défaillances importantes s'observent avec une panne soudaine d'ordinateur ou de serveur ou lorsque l'appareil semble défectueux. Un matériel compromis peut rendre les données incorrectes ou incomplètes, limiter ou supprimer l'accès aux données, ou compliquer l'utilisation des informations.

Mais il est possible de limiter les risques liés à l'intégrité des données en prenant quelques mesures :

- Limiter l'accès aux données et modifier les permissions ;
- Valider les données pour s'assurer qu'elles sont correctes quand elles sont collectées et utilisées par l'utilisateur final ;
- Effectuer une sauvegarde des données ;
- Utiliser des journaux pour suivre les ajouts, modifications ou suppressions de données ;
- Entreprendre régulièrement des audits internes ;
- Utiliser un logiciel de détection d'erreurs.

Après cette présentation de l'intégrité informationnelle, nous allons nous intéresser plus particulièrement aux risques rencontrés dans les transports maritimes, routiers et enfin ferroviaires.

C. Risques informationnels dans le secteur des transports

1. Le domaine des transports maritimes

L'espace maritime se situe au carrefour des enjeux internationaux, où la concurrence est exacerbée. Il est estimé à environ 50 000 le nombre de navires déployés[36]. Cette hypercompétitivité conduit à la généralisation de systèmes de suivi de navigation, tels que les radars marins, les satellites optiques ou radars à synthèse d'ouverture.

On peut citer comme exemple le Système d'Identification Automatique (AIS), système électronique qui permet aux navires d'envoyer et de recevoir des messages de positionnement, dans le but de prévenir des abordages ou de surveiller le trafic.

Cela se traduit aussi par la multiplication des angles d'attaques de nombreuses vulnérabilités. Parmi celles-ci, les plus critiques sont :

- La gestion de la cargaison. Celle-ci est de plus en plus digitalisée pour permettre aux armateurs d'améliorer leur gestion.
- Les outils de navigation sont-de plus en plus connectés avec des mises à jour via internet[37] (clé USB, disque dur externe, etc.). Une cyberattaque peut fausser les informations transmises ou rendre indisponible les outils de navigation (AIS, radar, etc.).
- Les systèmes de contrôle de la salle des machines (propulsion, production d'énergie).
- Les alarmes de sécurité et outils de surveillance.

La vulnérabilité des systèmes décrits ci-dessus est notamment sujette aux menaces suivantes :

- Vol des plans et des caractéristiques du bateau — piraterie, agression, détérioration du bateau (perturbations techniques), détournement, piratage des systèmes d'information ;
- Vol d'informations concernant la marchandise et sa valeur – vol de la marchandise, détérioration ;
- Vol d'informations concernant les clients — perte de crédibilité ;
- Vol d'informations sur les membres de l'équipage — atteinte à la sécurité ;

[36] « Cybersécurité : Évaluer et protéger les navires » Ministère de l'environnement de l'énergie et de la mer DGITM, Septembre 2016.

[37] Sachant que les passerelles non connectées sont également vulnérables aux virus via les systèmes de sauvegarde portatifs.

- Piratage des systèmes d'information.

Nous allons maintenant nous intéresser au AIS.

L'Organisation Maritime Internationale (OMI) l'a instauré en 2000 pour « *tous les navires de jauge brute supérieure ou égale à 300 engagés dans des voyages internationaux, les navires de charge de jauge brute supérieure ou égale à 500 et les navires à passagers, quel que soit leur tonnage*[38] ». Les transpondeurs sont utilisés pour envoyer des messages par ondes Very High Frequency (VHF)aux navires proches et aux stations côtières.

Toutefois, les messages envoyés par l'intermédiaire de l'AIS contiennent souvent des erreurs et subissent des falsifications ou un piratage, ce qui contribue à la perte de la qualité et de l'intégrité et de la confidentialité des données transmises[39]. Ainsi, environ 50 % des messages contiendraient des données erronées (informations fausses, incomplètes, etc.) et 1 % serait falsifié[40] (dégradation volontaire d'un message). Des acteurs extérieurs peuvent également créer de faux messages et les diffuser sur les fréquences AIS (piratage).

L'AIS n'est pas la seule technologie concernée. Une autre attaque consiste à viser un système de navigation alimenté par ordinateur : Electronic Chart Display (Ecdis). Cette technologie permet aux marins de substituer la carte papier par un système numérique. Une cyberattaque[41] a montré qu'il était possible de reconfigurer Ecdis pour tromper le système GPS. Elle usurpe la taille et l'emplacement des bateaux, ce qui déclenche faussement l'alarme de collision. Le département de cybersécurité du Royaume-Uni recommande d'utiliser des mots de passe forts et de tenir à jour les logiciels[42].

Par les exemples précités, il apparaît capital d'assurer la sécurité de ses informations afin de garantir la réussite de la mission.

2. Le domaine des transports routiers

En dix ans, le nombre de cyberattaques a été multiplié par sept, selon le rapport de la société israélienne upstream auto[43]. Cette augmentation pourrait s'expliquer par le développement massif d'applications télématiques dans les véhicules : gestion du trafic, du paiement électronique, de la gestion de fret et de flottes, de l'aide au conducteur et contrôle du véhicule[44].

[38] OMI, 2004.

[39] M, Badulzzi. « AIS Exposed Understanding Vulnerabilities & Attacks 2.0 », Trend Micro, 2014.

[40] Idem.

[41] L, Kellion. « Ship hack 'risks chaos in English Channel », BBC, 7/06/2018.

[42] « Code of Practice Cyber Security for Ships », Department of transport, 2017.

[43] «Rapid growth in cyber-attacks on smart mobility 2010-2019 », upstream, 19/05/2020.

[44] ISO/TR 14813-1, IS0, 2015.

Ces services télématiques s'appuient sur des technologies de la navigation, des télécommunications et de l'information géographique, mais leur intégration doit proposer une très haute qualité de service selon le type d'application.

À cet effet, la qualité des données collectées est primordiale : les techniques de localisation doivent être précises, les bases des données routières exhaustives, la géométrie routière doit être restituée de manière sensible et fiable (maitrise de la source de l'information géographique jusqu'à son exploitation finale).

Afin de garantir la qualité et l'actualité de ces géodonnées dans des applications qui se révèlent exigeantes, une étape de certification sera certainement nécessaire à moyen terme.

Cela demande parallèlement de pouvoir développer des instruments qui collectent l'information géographique en temps réel.

Cette mise en œuvre est en cours et a donné des résultats intéressants lors de l'utilisation de quelques applications d'aide à la conduite automobile (par exemple, pour l'alerte et le contrôle du véhicule en courbe).

L'analyse des cyberattaques a montré que la plupart des attaques ciblent[45] :

- Les porte-clés véhicules ;
- Les serveurs d'entreprise ;
- Les applications mobiles pour véhicules ;
- Les ports du véhicule.

Par ailleurs Waze a été victime d'une altération des données GPS utilisateur. Une personne a acheté quatre-vingt-dix-neuf téléphones d'occasion connectés à Google Maps. Il les a fait déplacer lentement, ce qui a simulé quatre-vingt-dix-neuf véhicules se déplaçant au même endroit à vitesse réduite. Waze a donc interprété ces informations comme étant un embouteillage[46].

Cet exemple nous montre qu'il est aisé de manipuler l'Intelligence Artificiel (IA). A Manhattan, des véhicules autonomes ont été piratés, ce qui a provoqué la collision des véhicules[47]. Aujourd'hui, le développement de la 5G favorise l'échange des communications intervéhicules.

[45] K, Hyatt. « New study shows just how bad vehicle hacking has gotten », Cnet, 18/12/2019.

[46] G, Ryckmans. « Google Maps : un artiste provoque un embouteillage virtuel en se promenant avec 99 smartphones », RTBF, 4 février 2020.

[47] J, Carter. « Hacked Driverless Cars Could Cause Collisions And Gridlock In Cities, Say Researchers », Forbes, 5/03/2019.

Ces flux posent des problèmes de sécurité pour l'utilisateur d'une part, et de sécurité de l'information (confidentialité, intégrité et disponibilité) d'autre part[48].

Les cyberattaques ne constituent pas uniquement le principal risque pour l'IA. L'expert interviewé nous rapportait également qu'il était possible de manipuler l'interprétation de l'IA, en modifiant les panneaux de signalisation. Il prenait l'exemple, en Iran, de personnes qui avaient collé des stickers sur un panneau stop, ce qui avait faussé l'interprétation de l'IA.

3. Le domaine des transports ferroviaires

La digitalisation du ferroviaire[49] concerne, certes, les passagers, mais affecte plus fondamentalement la dimension industrielle, pour l'ensemble des acteurs de la chaine de valeur :

- Les entreprises ferroviaires (opérateurs de transport de passagers et de fret) ;
- Les gestionnaires d'infrastructures ;
- Les constructeurs de matériels roulants ;
- Les fournisseurs d'équipements ferroviaires ;
- Les Entités en Charge de la Maintenance (ECM) ;
- Les entités publiques (organismes de régulation, autorités organisatrices des transports, etc.).

Afin de recueillir, transférer, traiter les données et fournir un réseau de communication pour tous les utilisateurs du ferroviaire, on utilise les Technologies de l'Information et de la Communication (TIC).

[48] Entretien expert en protection de l'information d'un groupe industriel du CAC 40 (voir compte-rendus d'entretiens).

[49] A, Drozhzhin. « Can you hack a train? », Kaspersky, 29/12/2015.

Ces TIC peuvent comprendre :

- Des capteurs pour les matériels roulants : surveillance des conditions d'utilisation (ouverture des portes, charge par essieu, vitesse, température des roulements, vibrations, etc.), surveillance des conditions extérieures (météo, température, etc.), moyens de localisation (GPS, accéléromètres, etc.) ;
- Des capteurs pour les infrastructures : vérification de l'usage et de l'état (position des aiguilles, nombre de trains ayant passé un point, etc.), conditions extérieures (météo, température, etc.) ;
- De la surveillance embarquée et au sol par caméra vidéo ;
- Des systèmes d'affichage et de communication de l'information (son, écrans, etc.) ;
- Des processeurs embarqués de traitement des données ;
- Des outils de diffusion des données à l'intérieur des trains, dans les gares ou au cœur des infrastructures (points d'accès WIFI, réseaux sans fil pour connecter les capteurs et les panneaux d'affichage) et des hubs de données pour la transmission des données à haute vitesse ;
- Des appareils mobiles, etc.

Ces outils produisent par conséquent une quantité importante de données dynamiques et permettent la communication entre des objets équipés de capteurs.

Mais la multiplicité des capteurs et des données en temps réel va générer de très nombreux flux et de très importants volumes de données. L'utilisation accrue de ces données pour les services utilisateurs et pour l'exploitation soulèvera la question de la confidentialité, de la sécurité et bien sûr de l'intégrité des données.

Dans le domaine ferroviaire, il est fréquent que l'attaquant pénètre le système d'information via le WIFI[50] pour, d'une part, accéder aux données personnelles des voyageurs et d'autre part, prendre le contrôle du train (système de freinage par exemple).

Les cybercriminels ciblent également les infrastructures critiques comme le système de contrôle et d'information ferroviaire. En Allemagne, les ordinateurs de la Deutsh Bahn ont été piratés. Ils ont été victimes d'un ransomware, où le message était affiché sur les écrans dans les stations (cf. **annexe 5 :** Attaque du ransomware NotPetya sur un affichage de la Deutsche Bahn).

Dans l'objectif de se prémunir contre les cyberattaques visant les infrastructures ferroviaires, un projet commun, « Honeytrain », a été lancé entre une société britannique et allemande. Ce projet permet d'analyser et de capitaliser sur les cyberattaques pour en tirer une stratégie nationale.

[50] K, Hall, « Hacking train Wi-Fi may expose passenger data and control systems », The Register, 11/05/2018.

Le projet a duré six semaines, pendant lesquelles il a été identifié 2 745 267 cyberattaques. La France comptait à elle seule, 7 % de ces dernières, ce qui la plaçait en troisième position (sur dix pays), derrière la Chine (41 %) et les États-Unis (9 %). Il est intéressant de noter que ces trois pays concentraient près des deux tiers des tentatives d'attaques.

Le respect de cette stratégie développera la résilience du domaine ferroviaire, ce qui s'inscrit dans la politique de cybersécurité de la France[51].

D. Disponibilité

Selon Cyber Edu, association conjointe entre l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), l'Université européenne de Bretagne et Orange, la disponibilité est la « Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues) » dans le domaine cyber.[52] La disponibilité de l'information est donc le degré d'accessibilité dans une structure donnée par une entité choisie (personne physique ou morale). Nous entendons ici la disponibilité de l'information comme le fait de pouvoir techniquement profiter de l'information à un instant précis en toute clarté. Il convient de s'interroger sur la digitalisation du transport et ses enjeux en termes de risques informationnels.

Selon le Comité National Routier (CNR), seuls 35 %[53] des sociétés françaises de transport routier longue distance de marchandises aurait recouru à des changes de Données Informatisées (EDI)[54] en 2018 (cf. **annexe 6 :** Système EDI). Ce système permet de fluidifier les transactions, de limiter les intermédiaires et donc d'assurer le bon échange des informations. La mise en place de ces systèmes d'information performants et générant une réelle plus-value nécessite un fort investissement, que les petites entreprises du transport de marchandises ne peuvent réaliser. Dans le transport routier les échanges se font alors de manière manuscrite, ce qui peut limiter l'activité des transporteurs.

1. La digitalisation du secteur du transport

La numérisation et la digitalisation du transport sont latentes, notamment dans le transport de marchandises. La fragmentation de ce secteur pose encore une fois des problèmes : l'investissement nécessaire pour digitaliser et faciliter les transactions et la supply chain en général est, par effet d'échelle, plus difficile à avancer pour les petites structures que les grands groupes. Il faut en effet environ 5 % des résultats annuels selon une étude PwC de 2016, pour

[51] « Revue stratégique de Cyberdéfense », SGDSN, 12/02/2018.

[52] « Sensibilisation et initiation à la cybersécurité », CyberEdu, 05/11/2015.

[53] Renaud CHASLE, « Digitalisation du TRM : Où en est-on vraiment ? », Transport Info, 11/02/2019

[54] Transfert de données entre systèmes d'information provenant d'utilisateurs de différents domaines (juridique, économique, commercial), fondé sur des normes matérielles et logicielles.

digitaliser une entreprise de transport. Capgemini estime que les entreprises réussissant leurs transitions numériques sont 26 % plus rentables que les autres.[55] C'est sur cette fragmentation du secteur et sur les profits qui attirent les entreprises que certains acteurs (notamment étrangers) jouent, en proposant des solutions de disponibilité d'information.

a. Le track & trace

La plupart des grandes entreprises de transport de marchandises (DHL, Kuehne + Nagel, Fedex, etc.) proposent des services de « track and trace » (suivi de marchandises). Ces systèmes de traçabilité reposent en grande partie sur des puces de radio-identification (RFID). Ces entreprises développent en général leurs propres services de traçabilité de marchandises, permettant l'accès à l'information en temps réel. L'information reste en interne et le cheminement de celle-ci est connu.

Les organismes plus petits n'ont pas cette chance. Ils préfèrent se tourner vers des entreprises tierces proposant ces services. Des acteurs comme Téléroute ou Timocom, également bourses de fret, donnent accès à ces services aux PME et Très Petites Entreprises (TPE). Ils sont respectivement belges et allemands. L'information du transporteur est partagée avec un tiers, sans conscience réelle des entreprises.

Le risque est d'autant plus important quand les informations sont transférées à un acteur hors de la juridiction du RGPD. Microsoft a ainsi ambitionné de lancer une solution de suivi en temps réel des camions en 2018, à l'aide des objets connectés.[56] Depuis, le géant américain a déployé les solutions « Fleet Tracker » (suivi de flotte de camions), « Truck Routing » (itinéraires des camions et GPS), « Distance Matrix » (Estimated Time of Arrival, prévision d'heure d'arrivée et optimisation des routes) à partir d' Application Programming Interface**s** (API) propres à Microsoft et des cartes Bing. Ces solutions, déployées par les transporteurs, rendent une information disponible pour le transporteur, mais également pour Microsoft. [57]

Cependant, selon un expert de la logistique chez un acteur majeur de la distribution sélective[58], la traçabilité n'est pas systématique dans le secteur du transport et ne s'applique que spécifiquement. La disponibilité de l'information n'est donc pas, dans tous les cas, nécessaire et ne s'applique qu'à des business cases qui requièrent cette traçabilité de marchandises. La blockchain peut, par exemple, être utilisée dans le transport agroalimentaire pour garantir la fraicheur des produits et éviter une contestation de la part du receveur.[59]

---

[55] Renaud CHASLE, « Digitalisation du TRM : où en est-on vraiment ? » Transport Info, 11/02/2019.

[56] « Microsoft s'intéresse au suivi de camions en temps réel », Actu Transport Logistique, 22 mai 2018.

[57] « Logistics and Fleet Management », Microsoft https://www.microsoft.com/en-us/maps/logistics.

[58] Interview d'un expert de la logistique effectuée le 13/05/2020.

[59] « Utiliser la blockchain dans sa chaîne logistique », Agro Media, 09/04/2020.

b. Les TMS et WMS

De même, les logiciels de gestion du transport et des entrepôts tels le Transport Management System (TMS) et Warehouse Management System (WMS) (cf. **Annexe 7 :** Représentation des systèmes TMS et WMS) sont coûteux à mettre en place et peu d'entreprises peuvent se targuer d'en posséder un en interne. Le groupe de vente de détail de mobilier Ikea en possédait un jusqu'à récemment avant de passer sous les systèmes d'Oracle.[60] Le géant de l'informatique propose en effet trois solutions, Oracle Transportation Management, Oracle Warehouse Management Cloud et plusieurs solutions de gestion du commerce international (bourse de fret et conformité). Unilever, DB Schenker, Kraft Foods et Fiat figurent parmi les utilisateurs de ces logiciels.[61] Ces solutions sont très utilisées puisque facilement interopérables avec d'autres applications de gestion du transport comme les applications de planification ou les CRM (Customer Relationship Management). Non seulement, les informations de la logistique peuvent être consultées par un acteur tiers étranger, mais la sécurité des données est en jeu : les informations étant stockées dans un cloud, elles peuvent être accessibles dans leur entièreté en cas de brèche dans la sécurité du fournisseur de logiciel.

c. La mutualisation des ressources dans le transport de marchandises : des remontées d'information simplifiées ?

Plusieurs transporteurs se regroupent parfois pour faciliter cette digitalisation en mutualisant les coûts et en restant maîtres de leurs technologies utilisées. L'interopérabilité des logiciels est également garantie puisque les logiciels de management du transport sont faits « sur mesure ». On peut citer le réseau ASTRE, FLO ou AXCIAL comme réseau de transporteurs mutualisant une bourse de fret et des outils de gestion du transport de marchandises. Les informations sont transmises entre membres du réseau, mutualisant parfois des EDI, notamment dans la messagerie.[62] Les fuites d'informations sont ainsi limitées.

2. La digitalisation, vectrice de vulnérabilités pour le transport ?

Selon Forbes, la complexité, la fragmentation du secteur et sa digitalisation rapide font du transport une cible prioritaire pour les attaques informationnelles. La rentabilité faible du secteur pousse aussi les acteurs à ne pas investir dans la cybersécurité[63]. Selon la Fédération des Industries Electriques, Electroniques et de Communication (FIEEC), fédération de syndicats professionnels membre du MEDEF, la digitalisation du transport ferroviaire amène une exposition croissante du secteur aux risques informationnels. En effet, Jochen Langheim, Vice-president Advanced Systems R&D Projects chez STMicroelectronics, a déclaré à l'occasion d'un rendez-vous

[60] Interview d'un expert de la logistique effectuée le 13/05/2020.

[61] Fiche ORACLE OTM, Supply Chain Magazine, 2014.

[62] Les Cahiers de l'Observatoire n° 178, Décembre 2001, CNR.

[63] Oliver WYMAN, « Time For Transportation & Logistics To Up Its Cybersecurity As Hackers Put It On Target List », Forbes, 28/06/2017.

de la fédération, que « L'arrivée des objets connectés a démultiplié les opportunités pour les hackers de prendre possession d'un objet. Il faut donc protéger à tous les niveaux ».[64] C'est pourquoi l'ANSSI a signé une lettre conjointe avec l'Établissement Public de Sécurité Ferroviaire (EPSF) en 2018, avec un accord « [prévoyant] un échange régulier d'informations entre les deux organisations concernant les incidents affectant la sécurité des systèmes d'information et un travail d'identification d'exigences de sécurité ferroviaire qui concerneraient les logiciels et équipements de communication ». Ces risques, clairement identifiés par les autorités, sont donc bien réels et surveillés.[65]

3. L'internet des objets

Pour rattraper son retard, le secteur emploie de plus en plus l'internet des objets pour acquérir de la donnée en temps réel.

Le transport est identifié par Forrester comme l'un des secteurs les plus utilisateurs d'internet des objets (IoT), représentant les discussions à distance entre capteurs. L'IoT permet de faciliter le parcours du voyageur dans le transport avec une information en temps réel, et la gestion du transport et des stocks dans le transport de marchandises. Son utilisation permet une disponibilité d'information accrue, accordant une vision plus précise des dysfonctionnements de la supply chain ou dans la fluidité des transports pour l'usager. L'IoT permet aussi de mettre en place une forme de maintenance prédictive (pneus connectés de Michelin[66], prévision des dysfonctionnements et prévention chez la SNCF[67] par exemple). CGI estime même que l'IoT transformera le transport routier jusqu'à l'automatiser et l'autonomiser.[68] Les bénéfices de l'IoT sont donc importants, notamment en termes de sécurité pour les transports publics de personnes (prévention des actes de malveillance, état du véhicule ou de la cargaison, affichage de messages sur la route pour la prévention d'accidents, etc.).[69]

Mais le développement trop rapide de l'IoT dans le transport amène également son lot de vulnérabilités. En effet, l'IoT, créant de nouvelles portes d'entrée sur des systèmes souvent interconnectés (pas de « silo » entre IoT et WMS ou TMS par exemple), les chaînes logistiques peuvent être plus exposées aux risques informationnels. Les dispositifs d'internet des objets

[64] « Ferroviaire : objectif cybersécurité », FIEEC, 17/09/2020.

[65] « Une coopération renforcée entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Établissement public de sécurité ferroviaire (EPSF) », ANSSI, 20/03/2018.

[66] Sylvain ARNULF, « Connecter 160 millions de pneus par an à l'horizon 2024, l'objectif (ambitieux) de Michelin », L'Usine Nouvelle, 27/11/2019.

[67] « L'IoT, une source complémentaire de données au service des opérations chez SNCF », # DigitalSNCF, 12/10/2018.

[68] Marie-Eve DECROOCQ-DUMAYET « Comment l'Internet des Objets améliore la gestion des transports urbains ? », CGI, 13/09/2016.

[69] « The Internet of Things in Transportation », Alcatel Lucent.

peuvent être mal configurés ou pas assez sécurisés, la cybersécurité n'étant pas la clé de voute du développement d'un tel outil.[70] Pour exemples :

- En novembre 2016, une attaque informatique touchant le métro de San Francisco a directement impacté les points de ventes de billets, forçant l'exploitant à rendre l'accès au métro gratuit pendant la durée de l'attaque. Le ransomware se serait propagé via des systèmes d'information Windows obsolètes. Des silos d'informations n'étant pas présents, il a pu se propager aux machines physiques.[71]
- En avril 2017, une mise à jour du système (et non pas une cyber-attaque)de la Rheinbahn, la compagnie de transports publics de Düsseldorf en Allemagne, s'est mal déroulée. 832 véhicules et 80 trajets ont été affectés. Les affichages ne fonctionnant plus, des panneaux ont dû être écrits à la main pour indiquer les départs et les itinéraires des transports.[72]
- En mai 2017, la Deutsche Bahn a été touchée par le ransongiciel Wannacry, affectant les dispositifs d'information de celle-ci.[73]
- En août 2017, des chercheurs de l'Université de Washington ont montré que des véhicules autonomes reposant sur l'IoT et l'utilisation massive de capteurs pouvaient être facilement « hackés », via de simples bandes noires ajoutées sur un panneau « STOP ». Le véhicule identifiait le nouveau panneau comme un panneau de limite de vitesse de 45 miles à l'heure (environ 72 km/h), pouvant créer des dommages inimaginables (cf. **annexe 8 :** Utilisation de bandes noires pour « hacker » les systèmes d'IoT des véhicules autonomes)[74].
- On peut également citer l'IoT embarqué des Tesla, à de multiples reprises compromis par des hackeurs chinois.[75] [76]

Les conséquences pourraient être dramatiques dans le cadre de réseaux interconnectés de véhicules. C'est pourquoi la protection de l'information doit parfois primer sur sa disponibilité.

L'IOT facilite la disponibilité de l'information, mais pas uniquement pour l'acteur qui met la solution en place ; elle peut également permettre un meilleur accès à l'information pour des personnes non autorisées et possiblement motivées par un but criminel. Sa mise en place doit

[70] Ibid.

[71] Harriet TAYLOR, « Metro transport systems eyed after hack attack in San Francisco », CNBC, 28/11/2016.

[72] Dirk NEUBAUER « Düsseldorf zwischen Update und Absturz: Schwarzer Donnerstag bei der Rheinbahn - Tausende kamen zu spät », Report-D, 20/04/2017.

[73] Chris GRAHAM, « Cyber-attack hits German train stations as hackers target Deutsche Bahn », The Telegraph, 13/05/2017.

[74] John BELTZ SNYDER « Researchers hack a self-driving car by putting stickers on street signs », Autoblog, 4/08/2017.

[75] Olivia SOLON, « Team of hackers take remote control of Tesla Model S from 12 miles away », The Guardian, 20/09/2016.

[76] Elizabeth WEISE, « Chinese group hacks a Tesla for the second year in a row », USA Today, 15/12/2019.

donc être faite dans un environnement cloisonné, où l'attaquant ne pourrait pas accéder au Système d'Information global de l'acteur concerné.

.

Partie III Etude de cas

Etude de Cas : Le Transport Maritime, Un long cheminement risqué pour une optimisation totale

Le transport maritime est un enjeu majeur de notre économie actuelle. Il représente un volume de 90 % d'échanges des marchandises mondiales. Les développements technologiques dans le transport, ainsi que l'évolution des relations politiques internationales, ont considérablement accru le commerce tant par sa taille que par sa portée. En effet, depuis les années 1900 jusqu'en 2014, ces échanges montrent un volume de 22 milliards d'euros de marchandises vendues, qui évolue à 61 milliards en 2014. Dans le monde, les exportations de produits manufacturés ont connu une augmentation de 3500 % de 1950 à 1998, ce qui montre une course au gigantisme des porte-conteneurs et plus largement une réelle demande de l'économie mondiale. [77]

La complexité du commerce maritime commercial mondial est mis en avant par ce commerce constamment croissant. Le nombre de porte-conteneurs et le nombre de données relatives constituent un volume aujourd'hui non négligeable dans la gestion des risques du transport maritime.[78]

Cette course du commerce maritime mondial n'est pas sans conséquences, bien qu'elle ait augmenté à un rythme plus lent depuis 2018[1] par rapports aux années précédentes, en raison de l'incertitude économique internationale et des guerres commerciales d'actualité. D'autant plus renforcé avec le contexte de guerre économique entre les Etats-Unis et la Chine, le transport maritime est sujet à la sensibilité de ses données. Notre étude de cas montrera les risques informationnels lié aux marchandises d'un conteneur naviguant d'un port à un autre. Nous aborderons également les solutions qu'envisagent les acteurs du secteur du transport maritime.

A. La protection des données, nouvel enjeu du secteur des transports

La cybersécurité se place au cœur de nombreux sujets de sécurité et la manipulation de données devient de plus en plus fréquente. Aujourd'hui, où l'information est une ressource, la manipulation de données peut donner un avantage concurrentiel en fournissant de nombreuses informations. Le transport maritime se voit de plus en plus exposé aux cyber-attaques dues aux évolutions technologiques en augmentation avec une aide électronique importante (par exemple : position du navire, navigation, communications, etc.)[79] et des équipages voués à être

[77] V. Saraogi, UNCTAD analyses impact of US-China trade war on shipping, Octobre 2019.

[78] C. J. Mc Mahon, Maritime Trade Warfare, Navar War College Review, volume 70, 2017.

[79] A. Biazetti, 5 key points about TradeLens platform security, Septembre 2019.

restreints. Le président de la commission des assurances transports, de la Fédération Française de l'Assurance (FFA), Patrick de la Morinerie, alerte sur cette nouvelle connectivité encore mal sécurisée sur les zones portuaires : « tout est connecté, les grues, les portiques, les ponts, les écluses, etc. ». Les assureurs craignent des cyberattaques qui pourraient causer des sinistres multiples à forte intensité. Le piratage des données des armateurs, des porte-conteneurs, des transporteurs et responsables portuaires pourrait être utilisé pour le vol de marchandises[80]. Ce risque souligne le besoin de cybersécurité lié à la disponibilité, l'intégrité, la confidentialité des informations.

Néanmoins, il ne s'agit pas du seul type d'attaque. Par exemple, le contexte récent a démontré des déstabilisations de grande ampleur sur l'intégrité des données avec l'attaque de ransomware comme « Not Petya »[81]. Un logiciel malveillant qui, une fois entré dans le réseau informatique, est capable de chiffrer toutes les données présentes sur un système d'information et d'engendrer une paralysie générale de l'activité d'une entreprise ciblée. Si ce même type d'attaque apparaissait dans une zone portuaire, une paralysie, même de courte durée, désordonnerait totalement les « supply chains » de plusieurs entreprises, et ce, de manière simultanée.

Il existe une multitude d'attaques plausibles dues à la numérisation et l'exploitation d'anciens systèmes d'informations, tels que le rançon-logiciel, l'usurpation d'identité, la falsification de données, la divulgation d'informations, le déni de service, ou encore l'élévation de privilège au sein d'un système d'information, afin de devenir omnipotent en tant qu'attaquant[82].

Les organisations ont, jusqu'à aujourd'hui, réagit aux changements drastiques dans les chaines d'approvisionnement, de différentes manières. Certains font pression sur les fournisseurs afin d'intégrer des systèmes communs pour obtenir une meilleure visibilité des marchandises. Pour les sous-traitants, certains utilisent encore des systèmes vieux de quarante ans pour intégrer et communiquer des informations comme le système EDI. Cette décision peut être liée à un manque de stratégie par ces acteurs, ou encore une peur de numériser toutes les informations car la transition n'est pas maitrisée, ou il n'y a pas l'expertise pour le faire. Bien que cette transition soit coûteuse, d'autres acteurs ont directement opté pour une solution numérique, avec un réseau spécialisé et sécurisé pour gérer des informations de manière précise. Grâce à l'analyse de données et parfois l'intelligence artificielle, certaines organisations sont devenues incroyablement sophistiquées dans leur capacité à comprendre leur environnement et savoir où se trouvent leurs marchandises. Cependant, cette construction de réseau sécurisé est incroyablement coûteuse (plusieurs millions d'euros) et l'acceptation des partenaires quant aux normes de conformité de sécurité imposées par ce type de système numérique est difficile.[83]

[80] H-M. Thomas, Le transport maritime face aux nouveaux risques, L'argus de l'assurance, 2015.

[81] M. Untersinger, Le virus Petya a coûté plus d'un milliard d'euros aux entreprises, Le Monde, 07/11/2017.

[82] A, Biazetti, « 5 key points about TradeLens platform security », Septembre 2019.

[83] S. Ciemcioch, « 3PL vs 4PL Logistics : Best Definition, Explanation and comparison », Warehouse Anywhere, Aout 2018.

Aujourd'hui les nouveaux enjeux de protections de données ciblent la transformation de flux d'informations vers les ports et les terminaux. C'est le type de défi que veut relever TradeLens, une entreprise émergente d'IBM qui travaille conjointement avec le mastodonte du transport Maersk. La solution apportée par TradeLens est celle d'une visibilité avancée provenant d'une plateforme favorisant plusieurs aspects de la chaine d'approvisionnement, dont l'optimisation des ports et des terminaux. Grossièrement, les informations seront structurées une fois reçue par le port en temps réel. Cela permettra à l'entité de continuer à recevoir des mises à jour de manière dynamique sur l'état de la réservation, des délais d'arrivée, des estimations ainsi que des modifications du plan de transport.[84]

En raison du nombre d'entités différentes impliquées dans le transport de marchandises pour aller à l'autre bout du monde, il existe une complexité inhérente aux coûts, imposée par les nouvelles technologies. Les systèmes actuels de communication et de maintien de la visibilité du fret ne sont pas suffisants pour assurer les chaînes d'approvisionnement complexes dont nous avons besoin aujourd'hui. Prenons comme exemple, la géolocalisation des porte-conteneurs entre deux ports qui assistent la navigation, fournissent une estimation sur l'horaire d'arrivée, et permettent d'éviter les collisions entre navires.

Les systèmes de données sur la navigation sont apportés par les satellites via le système GPS. Ces derniers peuvent être également soumis à des cyberattaques ou faire office d'espionnage économique par les données qui transitent via le satellite utilisé. L'anticipation d'un trajet, l'usurpation d'identité, la dégradation ou encore le blocage des services de positionnement, sont des risques palpables sur ce secteur. C'est en partie pourquoi chaque acteur majeur a développé ses propres satellites avec systèmes de géolocalisation par exemple. Le système pionnier reste le système américain « GPS », mais il existe aussi le système russe « Glonas », le système européen « Galileo », indien « NaviC », chinois « Beidou » et le système japonais « QZSS ». Le marché des appareils de repérage GPS devrait passer de 1,92 milliards d'euros en 2019, à environ 4 milliards d'euros en 2025. Le fret et les porte-conteneurs sont des facteurs principaux qui stimulent le marché des dispositifs de repérage par GPS [85] [86].

Les nouvelles solutions, notamment impliquant la géolocalisation, apportent un partage de données sécurisé, de manière structurée et permettent une visibilité complète du parcours d'un conteneur d'un bout à l'autre à travers toutes les parties prenantes impliquées. Le besoin croissant de dispositifs de suivi comme ceux utilisés pour la traçabilité ou les GPS appliqués au transport et à la logistique, souligne un réel besoin de protection des données.

[84] A. Pradi, « Ports and terminals: the missing element for full optimization », Tradelens, 2020.

[85] S. Singh, « GPS Tracking Device Market worth $3.7 billion by 2025 », Markets and Markets.

[86] N. Guibert, « La nouvelle guerre du GPS et ses risques », Le Monde, 02/05/2019.

B. La blockchain comme réponse aux problématiques de protection des données

Nous l'avons compris, les données ont une valeur. C'est pourquoi leur besoin de sécurité est plus que jamais une priorité dans l'élaboration stratégique des entreprises. Afin de se prémunir contre le risque d'altération des données, certaines entreprises du secteur des transports se sont tournées vers une alternative technologique récente, la blockchain.

Blockchain France définit la blockchain comme une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle[87]. En d'autres termes, il s'agit d'une base de données constituée de blocs (les nœuds), ayant chacun accès à une partie de l'information. Ces nœuds sont reliés entre eux, formant ainsi une chaîne. Cette chaîne permet de garantir la sécurité du système et donc la confidentialité et l'immuabilité des données ; c'est un réseau de confiance.

Inventé dès 2008, le concept de blockchain ne s'est réellement démocratisé que vers 2015[88]. Encore récente, cette technologie est peu connue des acteurs de petite taille qui ne sont pas familiers avec les problématiques de protection des données, mais elle devient de plus en plus un atout majeur pour les grandes entreprises.

1. Un système sécurisé

Pour comprendre précisément le fonctionnement de la blockchain, il est intéressant de comparer un système basique et un système de blockchain (cf. **Annexe 9 :** Schémas d'une blockchain classique dans la finance).

Dans l'exemple, le réseau de blockchain sécurise une transaction financière, mais le fonctionnement est exactement le même pour protéger des données. Supposons que Monsieur A veuille réaliser une transaction vers Madame B située à l'étranger. Sans la blockchain, cette transaction aurait nécessité l'intervention d'un ou plusieurs intermédiaires. Il y a donc un risque pour Monsieur A qu'il y ait une erreur dans la transaction ; qu'elle soit faite au profit de la mauvaise personne ou qu'il y ait une altération des données.

Dans le deuxième schéma, Monsieur A utilise la blockchain pour réaliser sa transaction au profit de Madame B. Dans cette situation, ce sont les utilisateurs de la blockchain qui vont transmettre la transaction sous forme de messages cryptés. Madame B recevra alors la somme convenue de la même façon qu'avant, mais entre-temps, celle-ci aura été décomposée pour être transmise par différents utilisateurs. Il n'y a pas d'intermédiaire, c'est pourquoi la blockchain est considérée comme un système décentralisé.

[87] « Qu'est-ce que la blockchain », Blockchain France.

[88] David Parkins, "The great chain of being sure about things", The Economist, 31/08/2015.

Dans le transport maritime, le fournisseur va transmettre les informations concernant sa commande (provenance, conservation, etc.) au deuxième maillon de la chaîne (le transporteur). En admettant que le message ait été transmis en utilisant une blockchain de dix nœuds, ce dernier recevra dix messages. Si l'un des utilisateurs a tenté de modifier l'information, le transporteur recevra neuf messages corrects et un message erroné. Il sera facile de savoir lequel est erroné, car chaque message transmis contient l'historique des modifications apportées à l'information initiale[89].

En outre, les données transmises dans la blockchain sont cryptées et les utilisateurs doivent utiliser, pour pouvoir transmettre la donnée, des clés de décryptage qui leur sont propres. Il n'est donc pas possible d'usurper l'identité d'un bloc, sans disposer des clés de décryptage.

2. Un système efficace

Outre la meilleure sécurisation des données qu'elle propose, la blockchain permet à l'entreprise un gain de productivité important. En supprimant le ou les intermédiaires, normalement présents dans le processus de transmission de l'information, cette dernière circule plus librement et plus rapidement.

Par ailleurs, il est possible d'automatiser la gestion des nœuds[90]. Ainsi, sur des critères objectifs, un algorithme peut vérifier automatiquement la véracité de l'information transmise. L'intervention humaine est alors complètement supprimée, effaçant le risque d'altération des données par l'homme. Cette automatisation permet de réduire le délai de traitement de l'information de plusieurs jours dans le cas où un intermédiaire vérifie l'information à quelques heures.

L'utilisation d'un système de blockchain présente de nombreux avantages et sa déclinaison dans la transmission de données permet d'améliorer la productivité de l'entreprise et de mieux protéger l'information transmise. Cette technologie pourrait donc être utilisée dans le secteur des transports afin de réduire les délais de traitement entre acteurs et d'améliorer la confiance dans un secteur dans lequel les intermédiaires sont très nombreux.

C. La démocratisation de l'outil dans le secteur des transports

Depuis le développement de la blockchain, celle-ci a été adaptée à beaucoup de secteurs. Son utilisation la plus connue est certainement la sécurisation de transactions entre banques. Pour autant, dans le secteur du transport maritime, cette technologie a été perçue comme une aubaine par beaucoup d'acteurs. Dans un secteur dans lequel les acteurs sont multiples, les avantages

[89] Loïc Le Gurun, « Blockchain et sécurisation des données », Force Plus, 28/06/2018.

[90] Joëlle Toledano, « Les enjeux de la blockchain », France Stratégie, juin 2018.

offerts par la blockchain sont nombreux et permettent notamment de réduire les coûts et délais de transport.

1. Un (trop) long processus de transport

Le processus de transport d'une marchandise fait intervenir plusieurs acteurs et chaque maillon de la chaine est potentiellement une cible d'attaque afin de récupérer des données. Le schéma ci-dessous (cf. Figure 8 : Présentation de Tradelens) montre un flux physique bref et concis tandis que le flux informationnel montre un volume d'information en augmentation depuis un client jusqu'à un fournisseur. Tout au long de la chaîne logistique, la marchandise transit par des moyens de transports de plus en plus restreints (Ex : entrepôt puis conteneurs sur navire puis camion et enfin destinataire) alors que le volume d'informations évolue de manière inversement proportionnelle au flux physique.

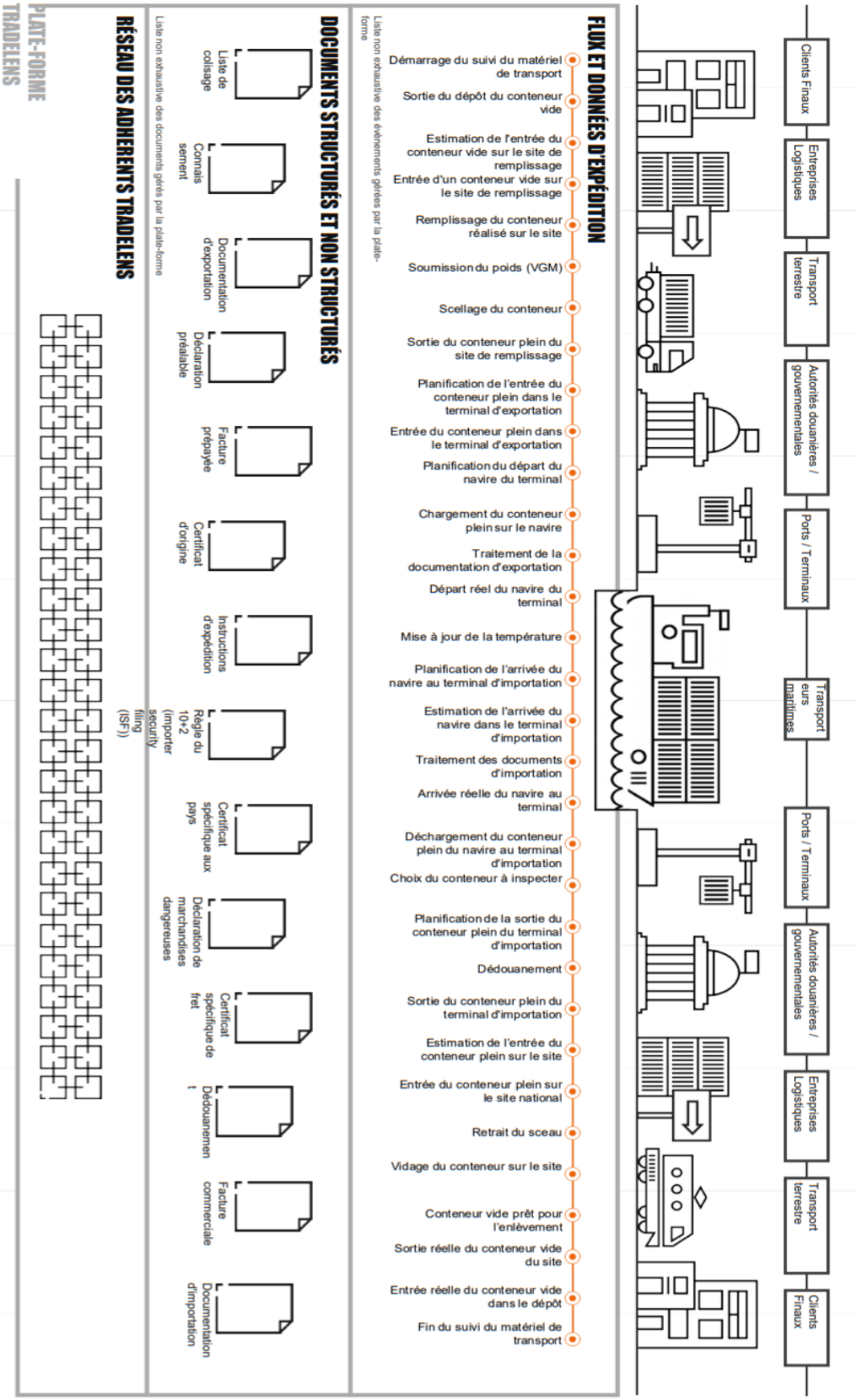


Figure 8 : Présentation de Tradelens (Source : B2E - 2020)

Au total, une dizaine d'acteurs interviennent du début de la production du produit à son acquisition par le client. Il s'agit notamment des opérateurs portuaires, des autorités, des transporteurs, des fournisseurs, des clients, des entreprises de logistique et des organismes bancaires et financiers.

La gestion et la sécurisation de la donnée tout au long de ce processus est un enjeu majeur pour les entreprises. Si l'on prend l'exemple du schéma ci-dessus, le client reçoit du transporteur 100 conteneurs mais déclare en avoir reçu seulement 99. En cas de contentieux entre deux parties, avoir pu tracer l'information permet d'apporter une solution à la problématique soulevée. Que ce soit une erreur humaine ou un acte de malveillance, il est important d'identifier les vulnérabilités de la chaîne d'approvisionnement et d'en apporter les correctifs.

En effet, pour limiter ce risque et pour garantir une traçabilité du produit, les acteurs du transport maritime réalisent aujourd'hui plus de trente contrôles tout au long de la chaîne de traitement[91]. Pour la plupart de ces contrôles, l'intermédiaire ouvre le conteneur, s'assure de la conformité du produit et de son adéquation avec les données transmises par l'expéditeur. Lorsqu'un écart est identifié, le conteneur est bloqué sur le lieu de contrôle jusqu'à vérification. Ces contrôles obligatoires sont notamment payants par les acteurs et représentent un cinquième des coûts du transport[92].

Pour le Boston Consulting Group, ces coûts et ces délais ne peuvent être réduits qu'à la seule condition que les acteurs collaborent entre eux pour créer un écosystème de confiance[93]. De plus, le Boston Consulting Group identifie neuf domaines pouvant être impactés positivement par la blockchain :

- Le manque de génération de données et de gestion des documents ;
- La gestion complexe de la conformité des flux & des équipements ;
- La complexité des procédures de paiement ;
- Le manque d'optimisation des flux & des flottes ;
- La gestion des documents de transport ;
- L'opacité des prix et des réservations ;
- La gestion des responsabilités en cas de litiges, plaintes ;
- La traçabilité des flux ;
- La reverse logistique.

Les problématiques identifiées semblent toutes converger vers un même problème : le manque de confiance entre acteurs. Afin de créer un écosystème de confiance, l'utilisation de la blockchain semble être la meilleure solution selon le Boston Consulting Group.

2. La blockchain permet-elle vraiment de créer un climat de confiance ?

[91] Samir Azizi, « La technologie blockchain au service du transport de conteneurs maritime ? » Transport Shaker - Wawestone, 17/05/2018.

[92] « Blockchain, logistique et supply chain : panorama des possibilités », Blockchain France, 23/08/2017.

[93] « Resolving the Blockchain Paradox in Transportation and Logistics », Boston Consulting Group, 29/01/2019.

La blockchain est particulièrement adaptée au secteur du transport maritime car elle permet aux utilisateurs de connaître tout l'historique de la donnée. Chaque acteur dispose en effet des mêmes informations. Du producteur au client, tous les acteurs connaissent les données d'expédition, la situation géographique du conteneur (GPS), la température de conservation des conteneurs, leur poids, leur origine, etc.[94] Il s'agit d'une véritable solution contre la fraude et la contrebande. Sans la blockchain, ces informations sont répertoriées uniquement sur papier la plupart du temps et vérifiées à chaque étape de la chaîne[95]. Le but est donc de transposer ces signatures sur un support informatique commun à tous. Ainsi, en cas de litige, il suffit simplement de se reporter à l'historique des modifications de la donnée dans la blockchain pour savoir si la donnée a été altérée. Il ne faut cependant pas oublier que cela fait apparaître un nouveau risque : la conservation et la gestion des données.

L'utilisation de la blockchain permettrait notamment la création de « smart contracts » : ce sont des algorithmes permettant d'automatiser certaines étapes du traitement de l'information[96]. Par exemple, il peut être configuré pour que lorsqu'un conteneur de produits dangereux est expédié, une assurance appropriée soit automatiquement souscrite.

Conscients de l'intérêt de la blockchain dans le secteur des transports, Maersk et IBM ont développé conjointement Tradelens, plus grande plateforme de blockchain pour le secteur maritime[97]. Ce sont ainsi près de vingt millions de conteneurs par an qui profitent de cette technologie. La force de ce réseau est qu'il fait intervenir l'ensemble des acteurs de la chaîne d'approvisionnement (listés dans la partie 3.1.)[98].

Si la blockchain semble être une solution aux coûts élevés et aux délais liés aux nombreux contrôles, les acteurs restent sceptiques sur l'utilisation de cette technologie, notamment car celle-ci fait intervenir d'autres acteurs. Le manque de confiance revient donc au cœur du sujet[99]. Le Boston Consulting Group a notamment réalisé un sondage afin d'évaluer la perception de la blockchain par les acteurs du transport. Sur le panel interrogé, seules 20 % des entreprises estiment que la blockchain figure parmi leurs dix priorités. 60 % des répondants pensent, quant à eux, que la blockchain n'est pas adaptée au secteur à cause du manque de coordination et de l'absence d'écosystème[100].

La blockchain peut donc être une solution pour améliorer la productivité, réduire les coûts et diminuer les délais de transport. Toutefois, pour que cette technologie puisse être utilisée, les acteurs devront réussir à s'entendre et à se coordonner.

---

[94] « La blockchain dans la logistique », BITO Systèmes.

[95] « Blockchain, logistique et supply chain : panorama des possibilités », Blockchain France, 23/08/2017.

[96] « Renault Chasle, Informatique transport : Qu'est-ce que la BlockChain ? », Transport Info, 25/06/2018.

[97] www.tradelens.com.

[98] « Présentation de Tradelens », Tradelens, 17/04/2019.

[99] "Resolving the Blockchain Paradox in Transportation and Logistics", Boston Consulting Group, 29/01/2019

[100] Mourad Krim, « Blockchain, les entreprises de transport et de logistique doivent intensifier leur collaboration », IT Social, 31/01/2019.

D. L'apparition de nouvelles problématiques

L'apparition de nouveaux référentiels en matière de sécurité rédigé par l'ANSSI commencent à être de plus en plus appliqués, notamment dans les organismes d'importance vitales (OIV). L'application de services de cybersécurité comme un centre de réponse à incident (CSIRT) ou encore d'un centre opérationnel de sécurité (SOC) permet de réagir rapidement face aux cybermenaces. Ces services deviennent des articulations incontournables pour assurer la sécurité d'un système d'information.

La formation d'expert est également à prendre en compte lors d'une transformation technologique. Bien que la technologie de la blockchain pourrait aider à sécuriser la chaine d'approvisionnement, le risque zéro n'existe pas puisque la place de l'Homme est encore importante dans la navigation du porte-conteneur. L'erreur humaine peut provenir de plusieurs manières comme la confiance excessive dans les outils de navigation, la fatigue, le défaut de management ou de culture de la sécurité. En 2019, l'analyse de près de 15 000 réclamations en responsabilité civile conduit à une facture de 1,5 milliards d'euros. Les assureurs estiment que cette marge va augmenter avec l'apparition d'outils plus complexes.[101]

Conclusion de l'étude :

Afin de sécuriser ces données, l'ensemble des acteurs du transport maritime doivent mettre à jour leurs systèmes pour se prémunir de ce nouveau type de sinistres. Ainsi de manière plus générale, ceux qui répondront le mieux au marché futur de la logistique sont les acteurs avec une stratégie de financement et d'investissement axée sur l'optimisation de la productivité. Les parties prenantes de l'ensemble de l'écosystème doivent travailler ensemble puisqu'ils sont dépendants les uns et des autres pour permettre aux flux d'informations de transiter, en optimisant les opérations et en améliorant ces communications en cascade avec toutes les entités impliquées dans ce flux de données. Comme dans de nombreux domaines, la coopétition entre les ports internationaux est la clé d'une chaîne logistique.

Une préoccupation demeure pour les acteurs du secteur quant à l'intégrité et la traçabilité des leurs propres informations et celles de leurs clients vers des plateformes numériques ;e qui pourrait les exposer à une nouvelle liste sinistre et de risques de sécurité très coûteux à combler. La blockchain est une technologie qui permet de répondre de manière sécurisée aux enjeux de la traçabilité, de l'intégrité, de la confidentialité et de la disponibilité. Néanmoins, elle ouvre la porte à de nouvelles cyberattaques encore mal maitrisées aujourd'hui.

[101] A. Descamps, Allianz : Une décennie de risques maritimes analysés, Journal de la Marine Marchande, 05/06/2019.

Conclusion

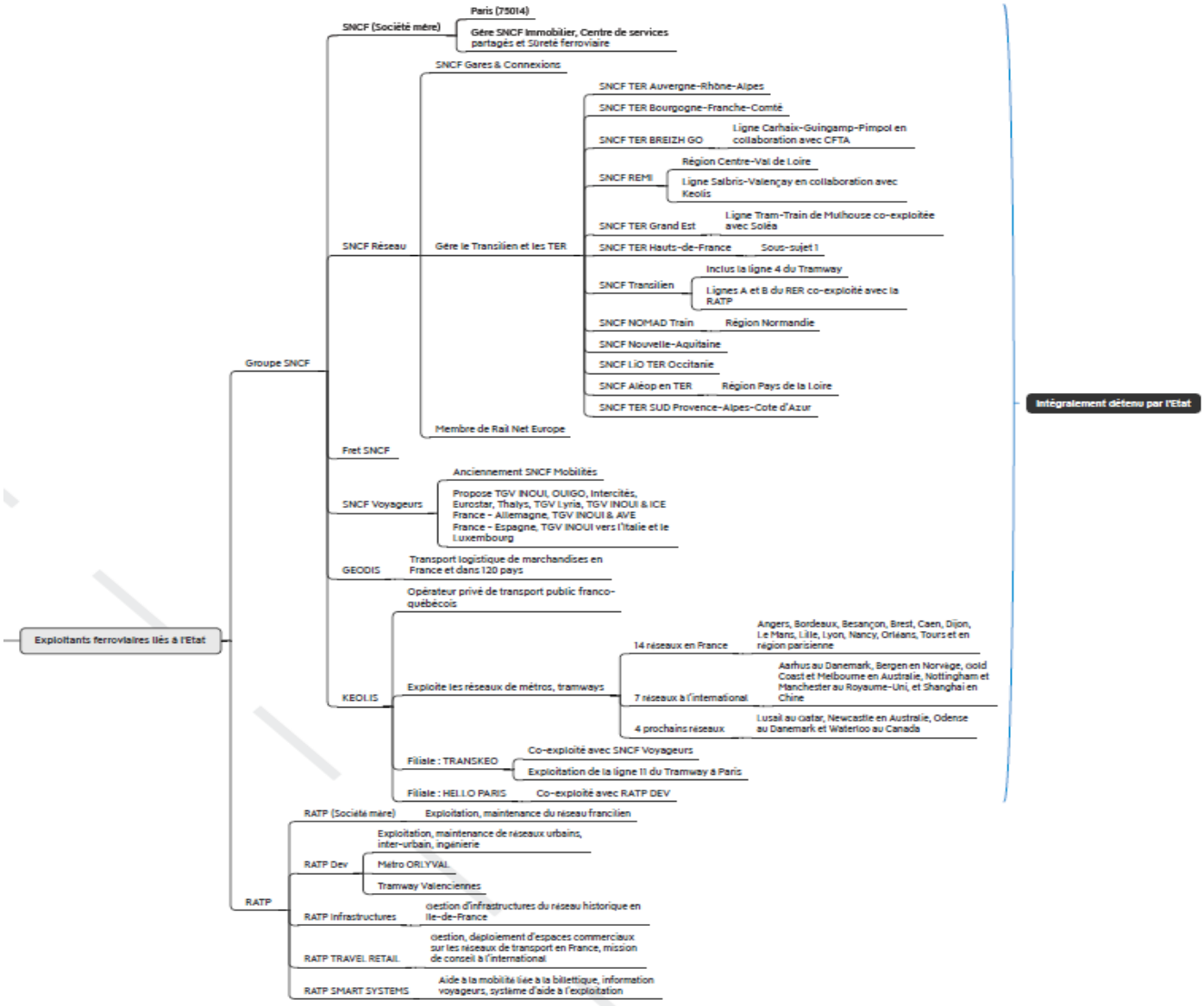
L'ouverture du transport aux nouvelles technologies est à double tranchant. Permettant un dynamisme du secteur via la plus grande disponibilité des données, elle amène aussi des problématiques de cybersécurité et de contrôle de l'information. En effet, l'intégration d'acteurs tiers dans la chaîne de données du transport peut amener à des pertes d'informations non désirées par les chargeurs, parfois au profit d'autres concurrents ou d'autres puissances. Mais ces risques sont peu visibles pour un secteur très fragmenté et extrêmement hétérogène. Pourtant, leurs impacts sont immenses, allant de l'espionnage industriel au sabotage de la chaîne logistique, entrainant à la fois une perte pour le transporteur, mais une perte encore plus importante pour le chargeur, qui doit alors subir les conséquences d'un risque qu'il ne maîtrise pas et qu'il ne peut pas maîtriser dans le cas d'un transport externalisé.

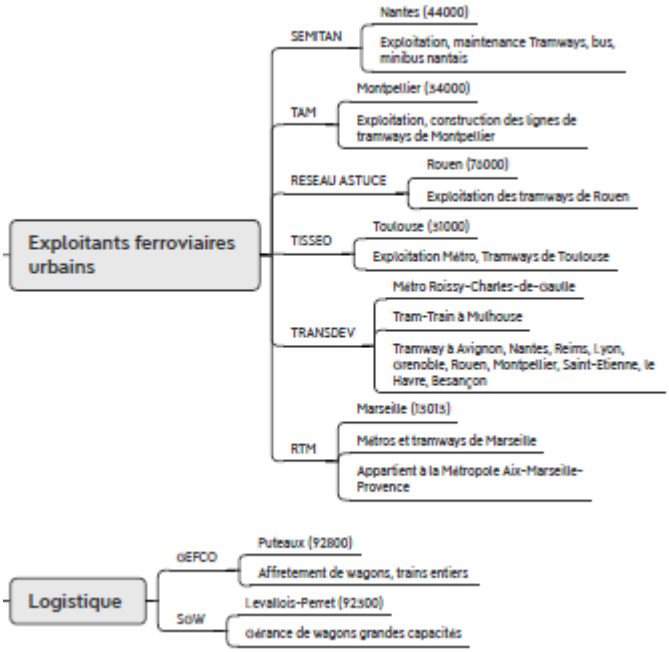
Il semble important et nécessaire pour le secteur, de prendre en compte les risques associés à sa digitalisation pour éviter d'apparaître comme un coût trop important pour le chargeur. Ces risques semblent d'autant plus importants lorsqu'ils sont dans le transport public, notamment de voyageurs, où les atteintes aux données envisageables peuvent avoir pour conséquence d'être désagréables au minimum, meurtrières au maximum. La prise de conscience du secteur n'est, pour l'instant, pas visible, même si de célèbres attaques (Maersk et NotPetya, Hacking de Tesla) ont déstabilisé l'ensemble du secteur.

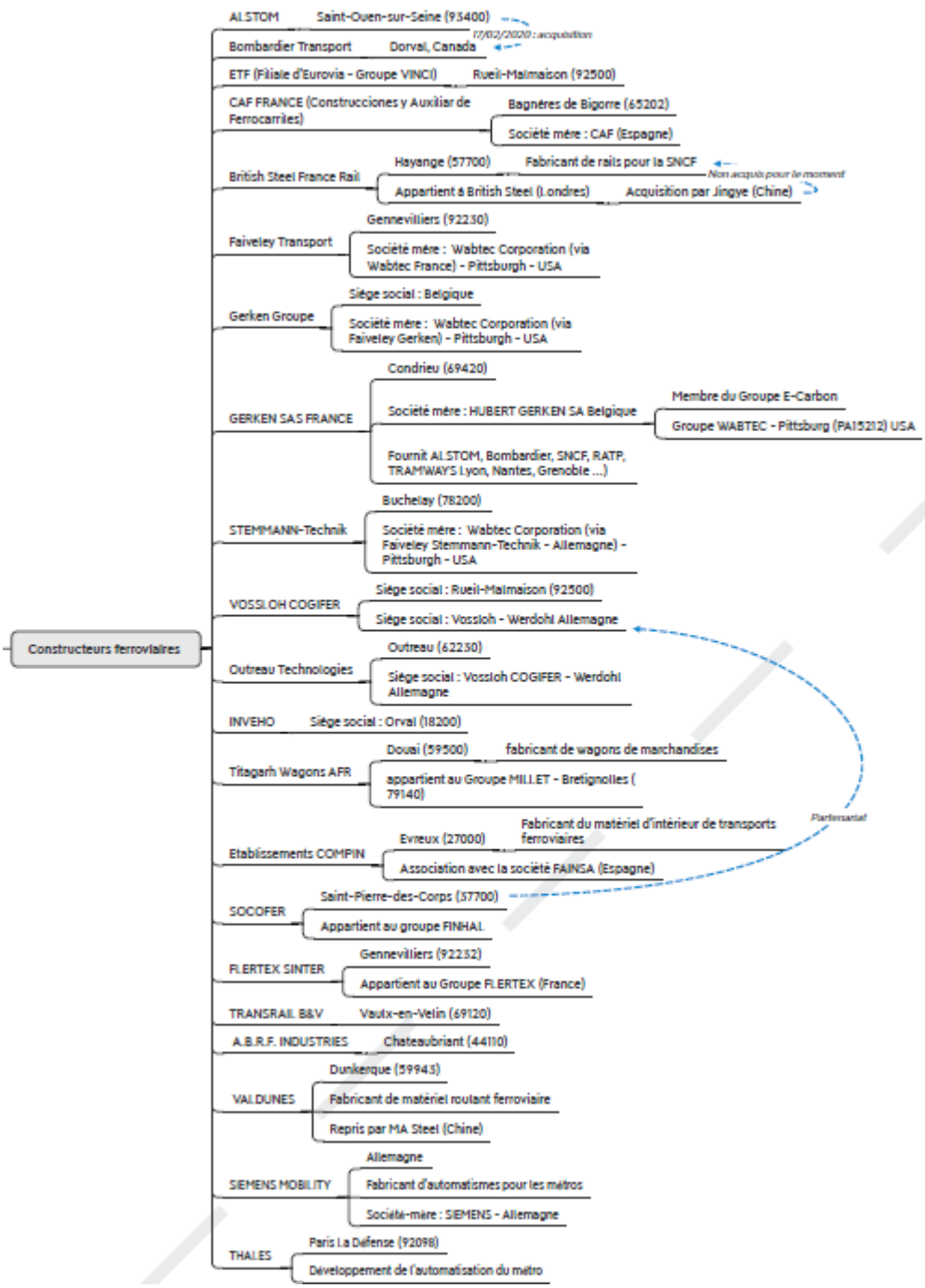
ANNEXES

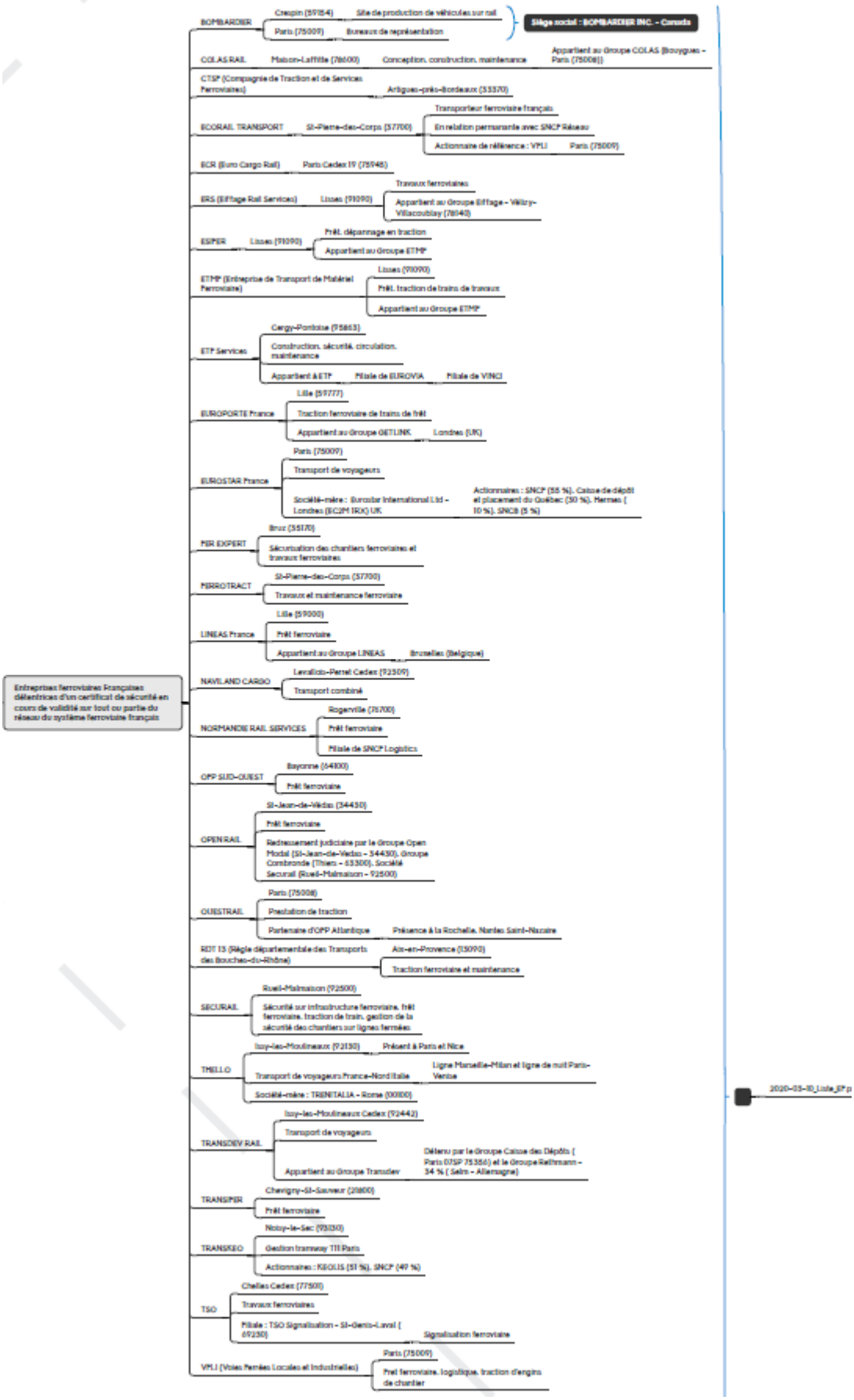
Annexe 1 : Cartographie du secteur ferroviaire français

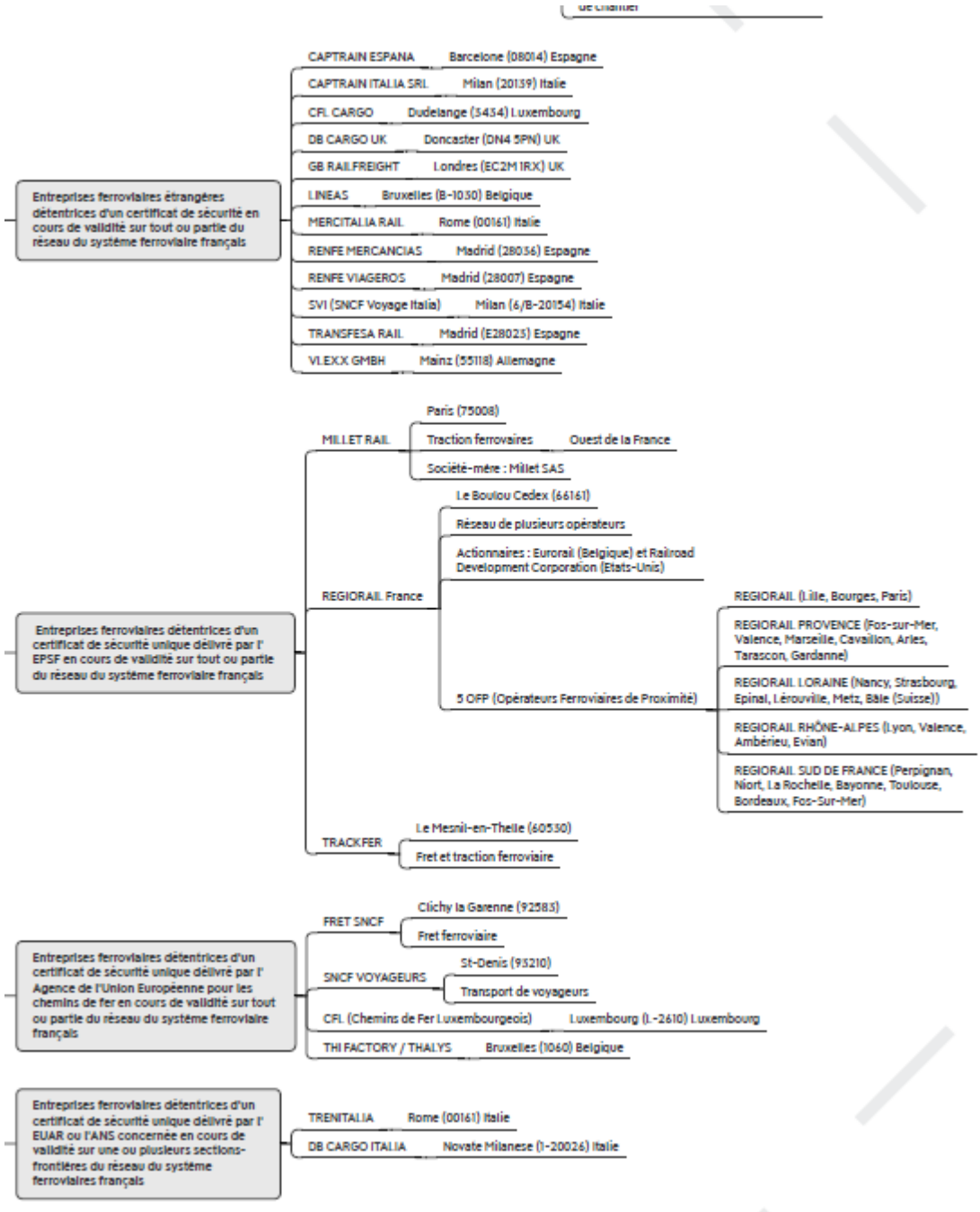
Fichier PDF	Fichier XMIND
Cartographie du secteur ferroviaire.p	Transports-ferroviaires.xmind

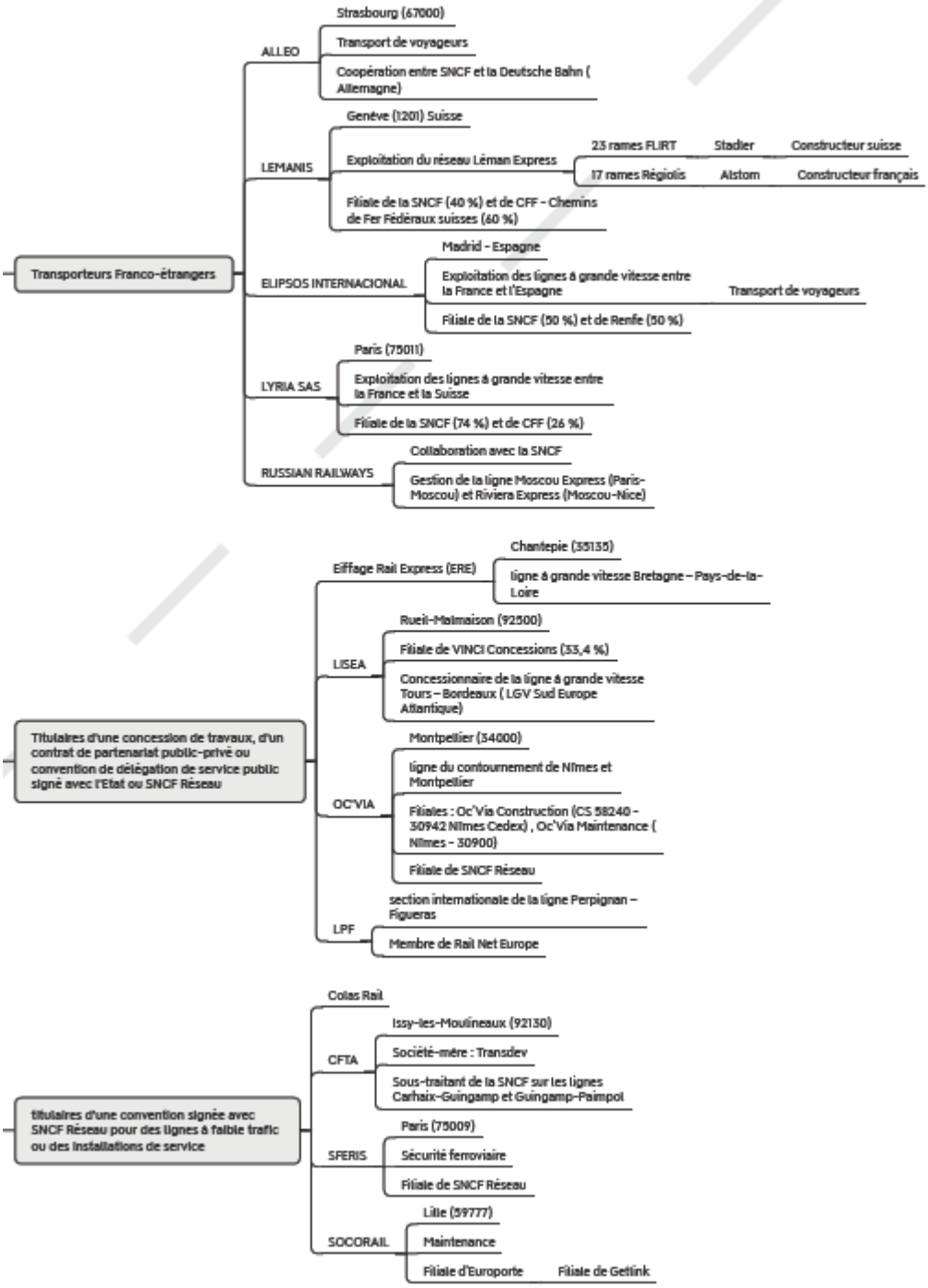


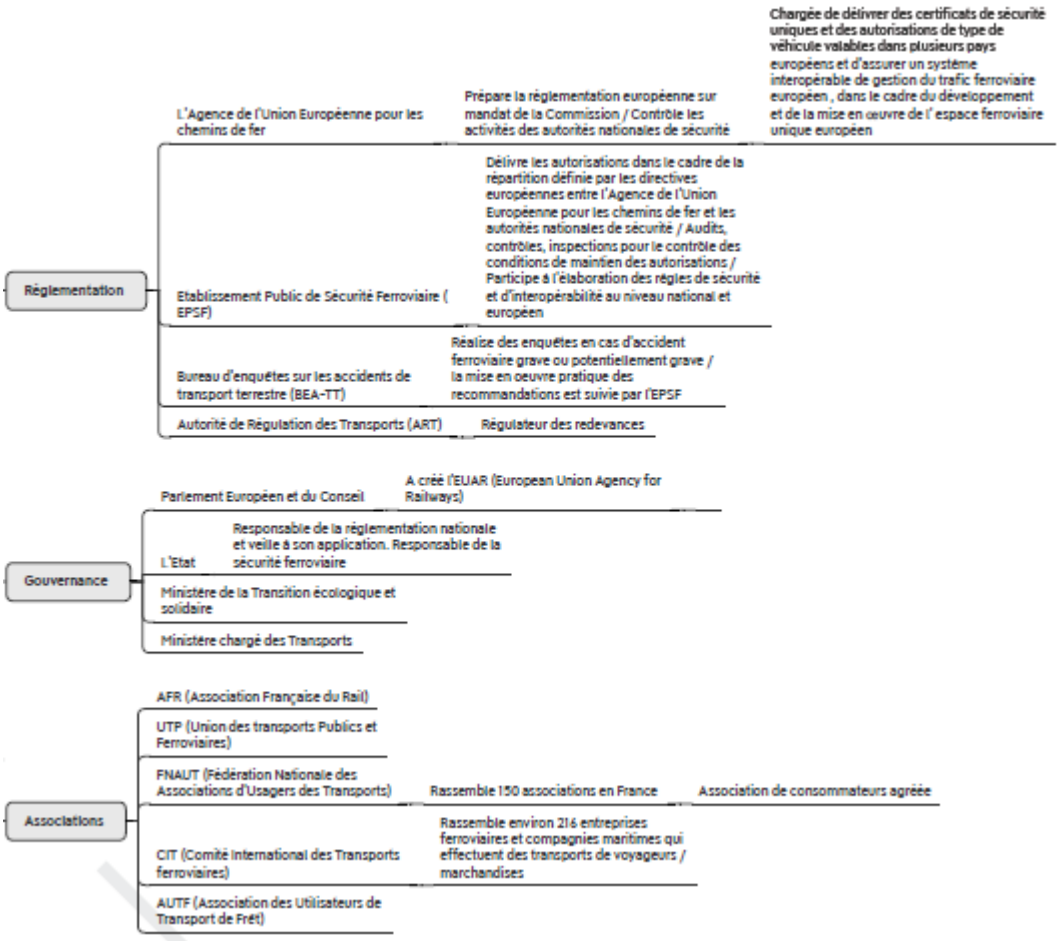

Exploitants ferroviaires urbains
SEMITAN
Nantes (44000)
Exploitation, maintenance Tramways, bus, minibus nantais
TAM
Montpellier (34000)
Exploitation, construction des lignes de tramways de Montpellier
RESEAU ASTUCE
Rouen (76000)
Exploitation des tramways de Rouen
TISSEO
Toulouse (31000)
Exploitation Métro, Tramways de Toulouse
TRANSDEV
Métro Roissy-Charles-de-Gaulle
Tram-Train à Mulhouse
Tramway à Avignon, Nantes, Reims, Lyon, Grenoble, Rouen, Montpellier, Saint-Etienne, le Havre, Besançon
RTM
Marseille (13013)
Métros et tramways de Marseille
Appartient à la Métropole Aix-Marseille-Provence
Logistique
VEFCO
Puteaux (92800)
Affretement de wagons, trains entiers
SOW
Levallois-Perret (92300)
Gérance de wagons grandes capacités


Constructeurs ferroviaires
ALSTOM
Saint-Ouen-sur-Seine (93400)
17/02/2020 : acquisition
Bombardier Transport
Dorval, Canada
ETF (Filiale d'Eurovia - Groupe VINCI)
Rueil-Malmaison (92500)
CAF FRANCE (Construcciones y Auxiliar de Ferrocarriles)
Bagnères de Bigorre (65202)
Société mère : CAF (Espagne)
British Steel France Rail
Hayange (57700)
Fabricant de rails pour la SNCF
Non acquis pour le moment
Appartient à British Steel (Londres)
Acquisition par Jingye (Chine)
Faiveley Transport
Gennevilliers (92230)
Société mère : Wabtec Corporation (via Wabtec France) - Pittsburgh - USA
Gerken Groupe
Siège social : Belgique
Société mère : Wabtec Corporation (via Faiveley Gerken) - Pittsburgh - USA
GERKEN SAS FRANCE
Condrieu (69420)
Société mère : HUBERT GERKEN SA Belgique
Membre du Groupe E-Carbon
Groupe WABTEC - Pittsburg (PA15212) USA
Fournit ALSTOM, Bombardier, SNCF, RATP, TRAMWAYS Lyon, Nantes, Grenoble ...)
STEMMANN-Technik
Buchelay (78200)
Société mère : Wabtec Corporation (via Faiveley Stemmann-Technik - Allemagne) - Pittsburgh - USA
VOSSLOH COGIFER
Siège social : Rueil-Malmaison (92500)
Siège social : Vossloh - Werdohl Allemagne
Outreau Technologies
Outreau (62230)
Siège social : Vossloh COGIFER - Werdohl Allemagne
INVEHO
Siège social : Orval (18200)
Titagarh Wagons AFR
Douai (59500)
fabricant de wagons de marchandises
appartient au Groupe MILLET - Bretignolles (79140)
Etablissements COMPIN
Evreux (27000)
Fabricant du matériel d'intérieur de transports ferroviaires
Association avec la société FAINSA (Espagne)
Partenariat
SOCOFER
Saint-Pierre-des-Corps (37700)
Appartient au groupe FINHAL
FLERTEX SINTER
Gennevilliers (92232)
Appartient au Groupe FLERTEX (France)
TRANSRAIL B&V
Vaulx-en-Velin (69120)
A.B.R.F. INDUSTRIES
Chateaubriant (44110)
VALDUNES
Dunkerque (59943)
Fabricant de matériel roulant ferroviaire
Repris par MA Steel (Chine)
SIEMENS MOBILITY
Allemagne
Fabricant d'automatismes pour les métros
Société-mère : SIEMENS - Allemagne
THALES
Paris La Défense (92098)
Développement de l'automatisation du métro


Entreprises ferroviaires françaises détentrices d'un certificat de sécurité en cours de validité sur tout ou partie du réseau du système ferroviaire français
BOMBARDIER
Crespin (59154) Site de production de véhicules sur rail
Paris (75009) Bureaux de représentation
Siège social : BOMBARDIER INC. – Canada
COLAS RAIL
Maison-Laffitte (78600) Conception, construction, maintenance
Appartient au Groupe COLAS (Bouygues – Paris (75008))
CTSP (Compagnie de Traction et de Services Ferroviaires)
Artigues-près-Bordeaux (33370)
ECORAIL TRANSPORT
St-Pierre-des-Corps (37700)
Transporteur ferroviaire français
En relation permanente avec SNCF Réseau
Actionnaire de référence : VPLI Paris (75009)
ECR (Euro Cargo Rail)
Paris Cedex 19 (75948)
ERS (Eiffage Rail Services)
Lisses (91090)
Travaux ferroviaires
Appartient au Groupe Eiffage – Vélizy-Villacoublay (78140)
ESPER
Lisses (91090)
Prél. dépannage en traction
Appartient au Groupe ETMF
ETMF (Entreprise de Transport de Matériel Ferroviaire)
Lisses (91090)
Prél. traction de trains de travaux
Appartient au Groupe ETMF
ETF Services
Cergy-Pontoise (75863)
Construction, sécurité, circulation, maintenance
Appartient à ETF Filiale de EUROVIA Filiale de VINCI
EUROPORTE France
Lille (59777)
Traction ferroviaire de trains de fret
Appartient au Groupe GETLINK Londres (UK)
EUROSTAR France
Paris (75009)
Transport de voyageurs
Société-mère : Eurostar International Ltd – Londres (EC2M 1RX) UK
Actionnaires : SNCF (55 %), Caisse de dépôt et placement du Québec (30 %), Hermes (10 %), SNCB (5 %)
MR EXPERT
Bruz (35170)
Sécurisation des chantiers ferroviaires et travaux ferroviaires
PERROTRACT
St-Pierre-des-Corps (37700)
Travaux et maintenance ferroviaire
LINEAS France
Lille (59000)
Prêt ferroviaire
Appartient au Groupe LINEAS Bruxelles (Belgique)
NAVELAND CARGO
Levallois-Perret Cedex (92309)
Transport combiné
NORMANDIE RAIL SERVICES
Rogerville (76700)
Prêt ferroviaire
Filiale de SNCF Logistics
OPP SUD-OUEST
Bayonne (64100)
Prêt ferroviaire
OPEN RAIL
St-Jean-de-Védas (34430)
Prêt ferroviaire
Redressement judiciaire par le Groupe Open Modal (St-Jean-de-Védas – 34430), Groupe Combronde (Thiers – 63300), Société Securail (Rueil-Malmaison – 92500)
OUESTRAIL
Paris (75008)
Prestation de traction
Partenaire d'OPP Atlantique Présence à la Rochelle, Nantes Saint-Nazaire
RDT 13 (Régie départementale des Transports des Bouches-du-Rhône)
Aix-en-Provence (13090)
Traction ferroviaire et maintenance
SECURAIL
Rueil-Malmaison (92500)
Sécurité sur infrastructure ferroviaire, fret ferroviaire, traction de train, gestion de la sécurité des chantiers sur lignes fermées
THELLO
Issy-les-Moulineaux (92130) Présent à Paris et Nice
Transport de voyageurs France-Nord Italie
Ligne Marseille-Milan et ligne de nuit Paris-Venise
Société-mère : TRENITALIA – Rome (00100)
TRANSDEV RAIL
Issy-les-Moulineaux Cedex (92442)
Transport de voyageurs
Appartient au Groupe Transdev
Détenu par le Groupe Caisse des Dépôts (Paris 07SP 75356) et le Groupe Rethmann – 34 % (Selm – Allemagne)
TRANSIMER
Chevigny-St-Sauveur (21800)
Prêt ferroviaire
TRANSKEO
Noisy-le-Sec (93130)
Gestion tramway TTI Paris
Actionnaires : KEOLIS (51 %), SNCF (49 %)
TSO
Chelles Cedex (77500)
Travaux ferroviaires
Filiale : TSO Signalisation – St-Denis-Laval (69230)
Signalisation ferroviaire
VPLI (Voies Privées Locales et Industrielles)
Paris (75009)
Prel ferroviaire, logistique, traction d'engins de chantier
2020-03-10_Liste_EF p


Entreprises ferroviaires étrangères détentrices d'un certificat de sécurité en cours de validité sur tout ou partie du réseau du système ferroviaire français
CAPTRAIN ESPANA Barcelone (08014) Espagne
CAPTRAIN ITALIA SRL Milan (20139) Italie
CFL CARGO Dudelange (3454) Luxembourg
DB CARGO UK Doncaster (DN4 5PN) UK
GB RAILFREIGHT Londres (EC2M 1RX) UK
LINEAS Bruxelles (B-1030) Belgique
MERCITALIA RAIL Rome (00161) Italie
RENFE MERCANCIAS Madrid (28036) Espagne
RENFE VIAGEROS Madrid (28007) Espagne
SVI (SNCF Voyage Italia) Milan (6/B-20154) Italie
TRANSFESA RAIL Madrid (E28025) Espagne
VLEXX GMBH Mainz (55118) Allemagne
Entreprises ferroviaires détentrices d'un certificat de sécurité unique délivré par l' EPSF en cours de validité sur tout ou partie du réseau du système ferroviaire français
MILLET RAIL
Paris (75008)
Traction ferroviaires Ouest de la France
Société-mère : Millet SAS
REGIORAIL France
Le Boulou Cedex (66161)
Réseau de plusieurs opérateurs
Actionnaires : Eurorail (Belgique) et Railroad Development Corporation (Etats-Unis)
5 OFP (Opérateurs Ferroviaires de Proximité)
REGIORAIL (Lille, Bourges, Paris)
REGIORAIL PROVENCE (Fos-sur-Mer, Valence, Marseille, Cavaillon, Arles, Tarascon, Gardanne)
REGIORAIL LORAINE (Nancy, Strasbourg, Epinal, Lérouville, Metz, Bâle (Suisse))
REGIORAIL RHÔNE-ALPES (Lyon, Valence, Ambérieu, Evian)
REGIORAIL SUD DE FRANCE (Perpignan, Niort, La Rochelle, Bayonne, Toulouse, Bordeaux, Fos-Sur-Mer)
TRACKFER
Le Mesnil-en-Thelle (60530)
Fret et traction ferroviaire
Entreprises ferroviaires détentrices d'un certificat de sécurité unique délivré par l' Agence de l'Union Européenne pour les chemins de fer en cours de validité sur tout ou partie du réseau du système ferroviaire français
FRET SNCF
Clichy la Garenne (92583)
Fret ferroviaire
SNCF VOYAGEURS
St-Denis (93210)
Transport de voyageurs
CFL (Chemins de Fer Luxembourgeois) Luxembourg (L-2610) Luxembourg
THI FACTORY / THALYS Bruxelles (1060) Belgique
Entreprises ferroviaires détentrices d'un certificat de sécurité unique délivré par l' EUAR ou l'ANS concernée en cours de validité sur une ou plusieurs sections-frontières du réseau du système ferroviaires français
TRENITALIA Rome (00161) Italie
DB CARGO ITALIA Novate Milanese (I-20026) Italie


Transporteurs Franco-étrangers
ALLEO
Strasbourg (67000)
Transport de voyageurs
Coopération entre SNCF et la Deutsche Bahn (Allemagne)
LEMANIS
Genève (1201) Suisse
Exploitation du réseau Léman Express
23 rames FLIRT
Stadler
Constructeur suisse
17 rames Régiolis
Alstom
Constructeur français
Filiale de la SNCF (40 %) et de CFF - Chemins de Fer Fédéraux suisses (60 %)
ELIPSOS INTERNACIONAL
Madrid - Espagne
Exploitation des lignes à grande vitesse entre la France et l'Espagne
Transport de voyageurs
Filiale de la SNCF (50 %) et de Renfe (50 %)
LYRIA SAS
Paris (75011)
Exploitation des lignes à grande vitesse entre la France et la Suisse
Filiale de la SNCF (74 %) et de CFF (26 %)
RUSSIAN RAILWAYS
Collaboration avec la SNCF
Gestion de la ligne Moscou Express (Paris-Moscou) et Riviera Express (Moscou-Nice)
Titulaires d'une concession de travaux, d'un contrat de partenariat public-privé ou convention de délégation de service public signé avec l'Etat ou SNCF Réseau
Eiffage Rail Express (ERE)
Chantepie (35135)
ligne à grande vitesse Bretagne – Pays-de-la-Loire
LISEA
Rueil-Malmaison (92500)
Filiale de VINCI Concessions (33,4 %)
Concessionnaire de la ligne à grande vitesse Tours – Bordeaux (LGV Sud Europe Atlantique)
OC'VIA
Montpellier (34000)
ligne du contournement de Nîmes et Montpellier
Filiales : Oc'Via Construction (CS 58240 - 30942 Nîmes Cedex) , Oc'Via Maintenance (Nîmes - 30900)
Filiale de SNCF Réseau
LPF
section internationale de la ligne Perpignan – Figueras
Membre de Rail Net Europe
titulaires d'une convention signée avec SNCF Réseau pour des lignes à faible trafic ou des installations de service
Colas Rail
CFTA
Issy-les-Moulineaux (92130)
Société-mère : Transdev
Sous-traitant de la SNCF sur les lignes Carhaix-Guingamp et Guingamp-Paimpol
SFERIS
Paris (75009)
Sécurité ferroviaire
Filiale de SNCF Réseau
SOCORAIL
Lille (59777)
Maintenance
Filiale d'Europorte
Filiale de Getlink

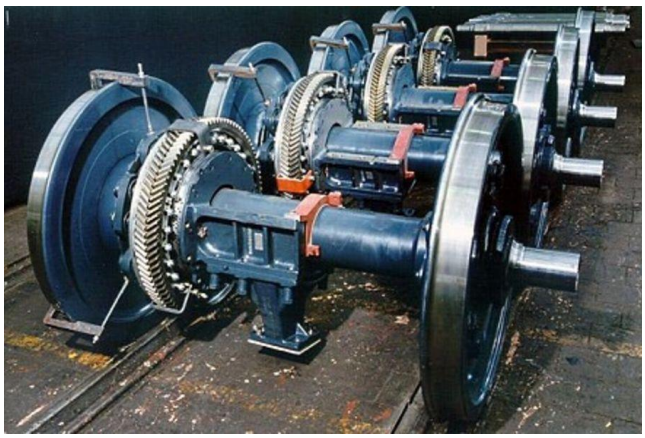

Réglementation
L'Agence de l'Union Européenne pour les chemins de fer
Prépare la réglementation européenne sur mandat de la Commission / Contrôle les activités des autorités nationales de sécurité
Chargée de délivrer des certificats de sécurité uniques et des autorisations de type de véhicule valables dans plusieurs pays européens et d'assurer un système interopérable de gestion du trafic ferroviaire européen , dans le cadre du développement et de la mise en œuvre de l' espace ferroviaire unique européen
Etablissement Public de Sécurité Ferroviaire (EPSF)
Délivre les autorisations dans le cadre de la répartition définie par les directives européennes entre l'Agence de l'Union Européenne pour les chemins de fer et les autorités nationales de sécurité / Audits, contrôles, inspections pour le contrôle des conditions de maintien des autorisations / Participe à l'élaboration des règles de sécurité et d'interopérabilité au niveau national et européen
Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT)
Réalise des enquêtes en cas d'accident ferroviaire grave ou potentiellement grave / la mise en oeuvre pratique des recommandations est suivie par l'EPSF
Autorité de Régulation des Transports (ART)
Régulateur des redevances
Gouvernance
Parlement Européen et du Conseil
A créé l'ELIAR (European Union Agency for Railways)
L'Etat
Responsable de la réglementation nationale et veille à son application. Responsable de la sécurité ferroviaire
Ministère de la Transition écologique et solidaire
Ministère chargé des Transports
Associations
AFR (Association Française du Rail)
UTP (Union des transports Publics et Ferroviaires)
FNAUT (Fédération Nationale des Associations d'Usagers des Transports)
Rassemble 150 associations en France
Association de consommateurs agréée
CIT (Comité International des Transports ferroviaires)
Rassemble environ 216 entreprises ferroviaires et compagnies maritimes qui effectuent des transports de voyageurs / marchandises
AUTF (Association des Utilisateurs de Transport de Fret)

Annexe 2 : Article de Usine Nouvelle sur la reprise de Valdunes par MA Steel

Le chinois MA Steel reprend Valdunes

02/06/2014

Le tribunal de commerce de Valenciennes (Nord) a choisi l'offre proposée par le chinois MA Steel pour reprendre les actifs du sous-traitant ferroviaire Valdunes. Celui-ci s'engage à maintenir les effectifs (487 emplois) des sites de Trith-Saint-Léger et Leffrinckoucke dans le Nord.



GHH-Valdunes fournit les axes, roues et essieux-montés des engins ferroviaires de traction.© GHH-Valdunes

Sur les quatre offres de reprise du sous-traitant ferroviaire Valdunes, une seule avait le soutien des syndicats : celle déposée par le chinois MA Steel. Elle a également convaincu le tribunal de commerce de Valenciennes (Nord), et ce pour une raison majeure : elle permet le maintien des 487 emplois sur les deux sites concernés, à Trith-Saint-Léger et Leffrinckoucke, situés respectivement près de Valenciennes et Dunkerque, dans le Nord.

Emplois maintenus et investissements à venir

MA Steel annonce la reprise de la totalité des actifs et une série d'investissements d'un montant de 50 millions d'euros sur cinq ans destinés à la modernisation de l'outil de production. Mais l'atout du nouveau repreneur est également d'apporter ce qui a tant manqué à Valdunes jusqu'à présent : l'intégration dans un groupe sidérurgique et une ouverture internationale.

MA Steel, créé en 1958, est un groupe sidérurgique coté en bourse en Chine. Il est spécialisé dans la fabrication de produits plats, de produits longs, d'aciers spéciaux et de roues ferroviaires (une structure qui ressemble étonnamment à celle d'Usinor Denain-Trith Saint-léger, avant son démantèlement et la création d'une part de Valdunes et d'autres part d'Ascométal). Détenant 80 % des parts de marché des roues ferroviaires en Chine, il dispose de trois filiales internationales : Maanshan Iron and Steel Co (Australie), Maanshan Iron and Steel Co. Ltd (Hong-Kong), et MG Allemagne développement Co.Ltd. Il affiche, pour l'année 2012, un chiffre d'affaires de 9 milliards d'euros, et emploie 41 220 salariés.

Un centre de R&D pour les produits ferroviaires

Intégrée au groupe MA Steel, Valdunes - dénommée maintenant MG Valdunes - va pouvoir présenter sa technologie sur le marché chinois du TGV (en neuf, et en réparation) et sur celui des marchés du métro et du tramway en Europe. L'industriel nordiste va également bénéficier du transfert de production de plus de 10 000 roues sur les 700 000 roues fabriquées par MA Steel et destinées jusqu'alors au marché européen. Enfin, MA Steel a annoncé la création, au sein de MG Valdunes, d'un centre recherche et de développement pour les produits ferroviaires. Ce dernier devrait activement participer aux programmes du pôle de compétitivité ferroviaire e-trans mis en place dans la région du Nord-Pas de Calais.

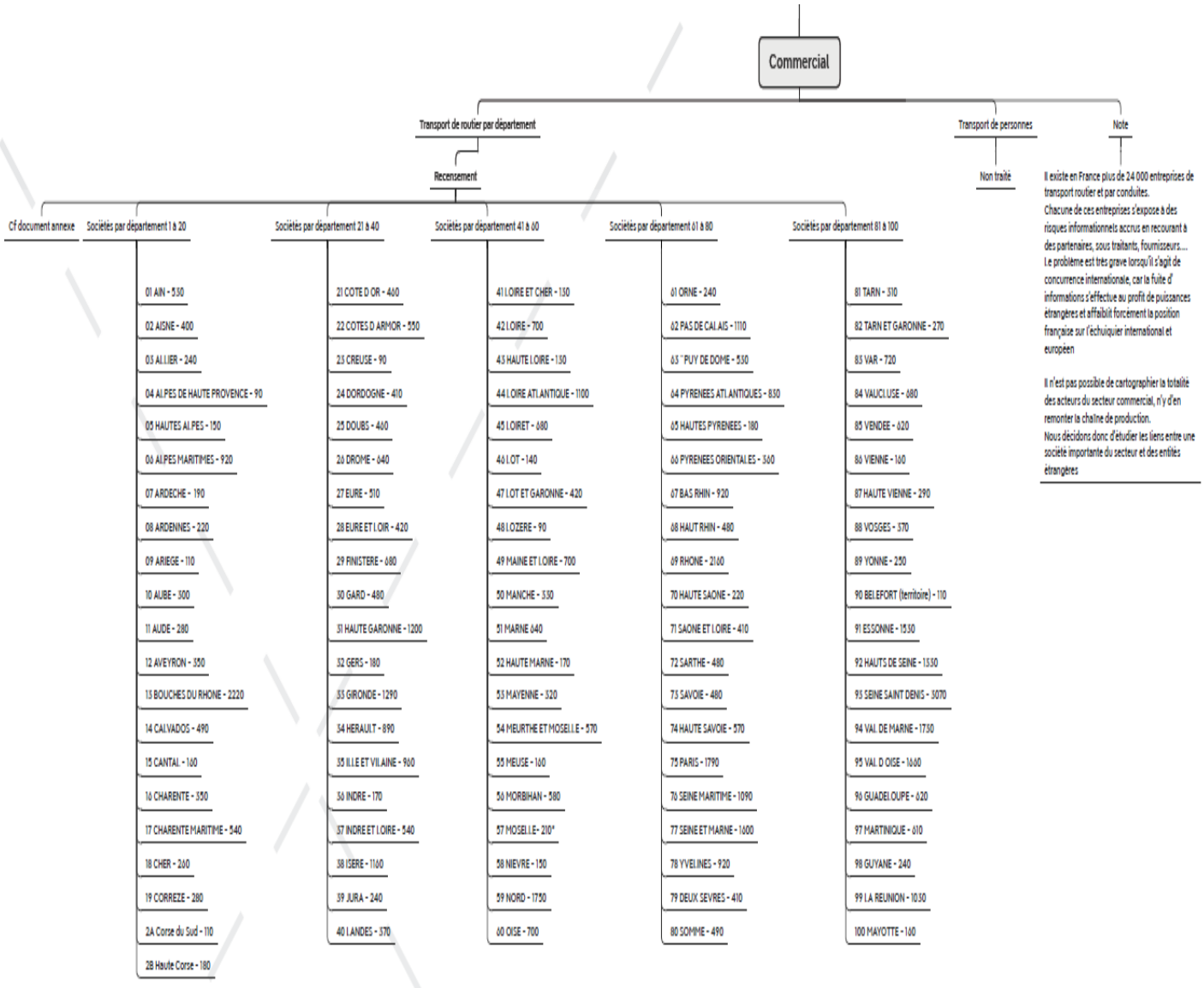
Spécialisée dans la fourniture et la maintenance d'axes, de roues et d'essieux montés, destinés à la fois au transport ferroviaire et urbain (métro), Valdunes avait été placé en redressement judiciaire le 1er avril. Il

était détenu par GHH Radsatz International, la société holding du groupe GHH-Valdunes, elle-même contrôlée par le fonds d'investissement Syntegra Capital. Outre les sites de Leffrinckoucke et de Trith-Saint-Léger près de Valenciennes, GHH Valdunes compte également un site à Oberhausen (en Allemagne) et un autre à Liège (en Belgique).

Francis Dudzinski

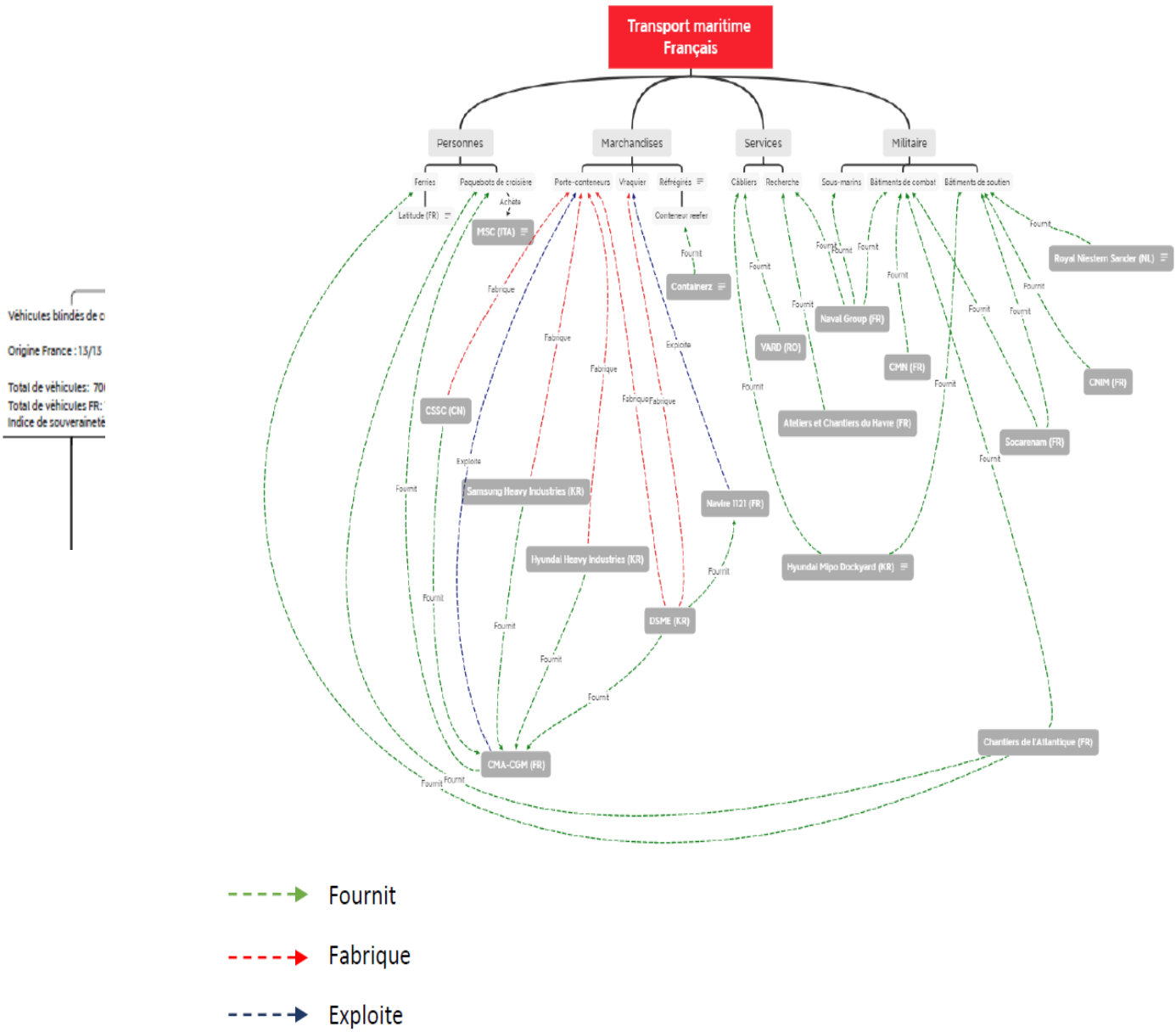
Annexe 3 : Cartographie du secteur routier français

Fichier PDF	Fichier XMIND
Transport-Routier.pdf	Transport-Routier.xmind



Annexe 4 : Cartographie du secteur maritime français

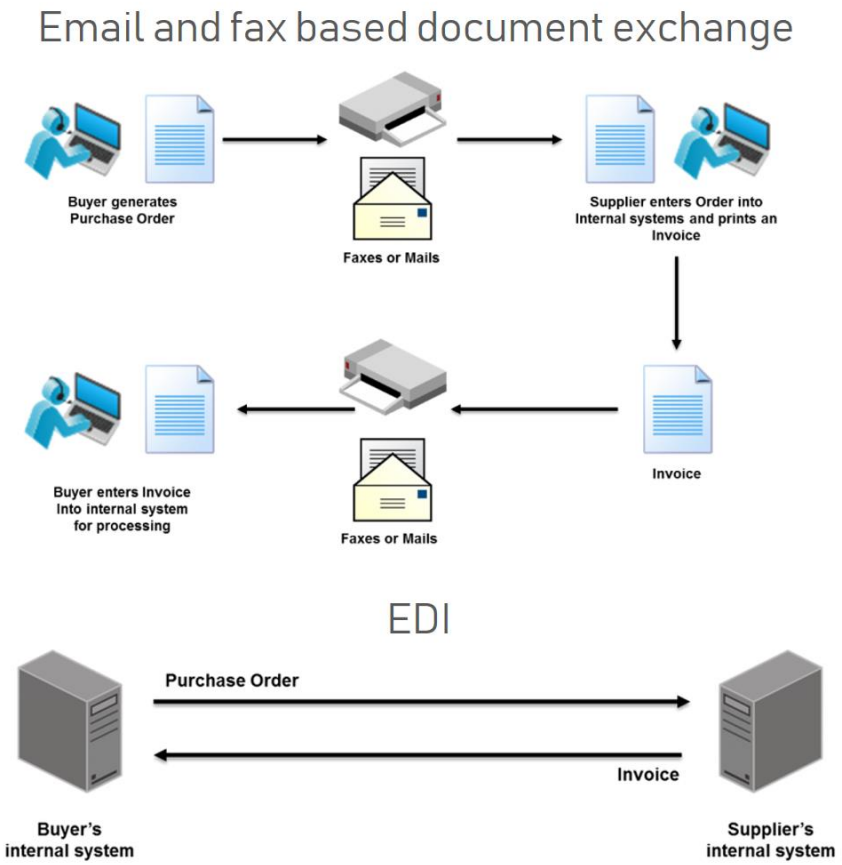
Fichier PDF	Fichier XMIND
Transport Maritime.pdf	Transport-maritime-Français.xmind



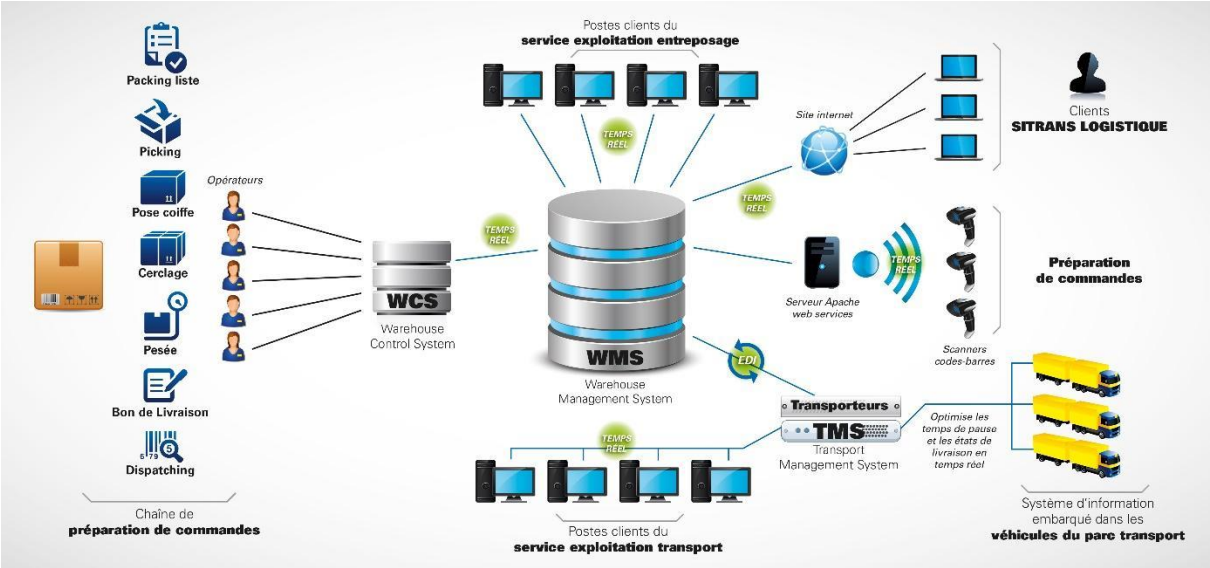
Annexe 5 : Attaque du ransomware NotPetya sur un affichage de la Deutsche Bahn

Source : Telegraaf.nl

Annexe 6 : Système EDI



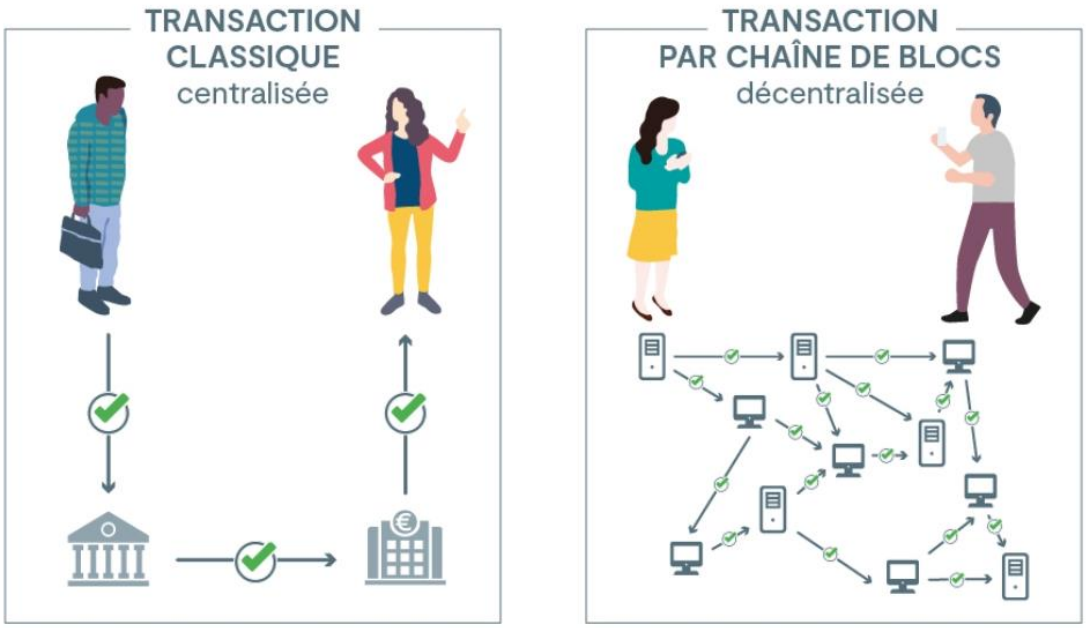
Annexe 7 : Représentation des systèmes TMS et WMS



Source : Sitrans.fr

Annexe 8 : Utilisation de bandes noires pour « hacker » les systèmes d'IoT des véhicules autonomes

Annexe 9 : Schémas d'une blockchain classique dans la finance



Source : www.economie.gouv.fr

COMPTE-RENDUS D'ENTRETIENS

Compte-rendu de l'entretien d'un expert en protection de l'information d'un groupe industriel du CAC 40

MM. Nicolas Ragot et Benjamin Roman ont réalisé un entretien le 12 mai 2020 dans le cadre d'une étude sur le risque informationnel dans le secteur des transports. L'expert, que nous appellerons M Ronand, a exprimé la volonté de conserver son anonymat de même que celui de la société.

L'interview s'est construite sur la base des questions suivantes :

- Pouvez-vous présenter succinctement votre parcours et votre fonction ?
- Qu'est-ce qui a motivé votre entreprise à créer une direction de la protection de l'information ?
- Que représente le risque informationnel dans un grand groupe tel que le vôtre ?
- Quelles peuvent être les mesures prises pour garantir la protection des informations (blockchain par exemple) ?
- Quels sont les enjeux de l'innovation technologique dans la garantie de la protection de l'information pour les véhicules de plus en plus autonomes ?
- Pouvez-vous nous raconter une anecdote sur un évènement ayant eu un impact sur la confidentialité / intégrité / disponibilité de l'information ?

M Ronand, diplômé en sécurité des réseaux et des télécoms a d'abord commencé sa carrière dans la protection des systèmes d'informations dans le secteur assurantiel, informatique puis dans le transport. Il occupe maintenant la fonction de responsable de la protection de l'information, qui est un département appartenant à la direction de la sûreté groupe. La sécurité est répartie dans trois autres directions, l'informatique, les véhicules connectés et la SSI. Le département de la protection des informations a été développé à la suite d'un scandale qui a démarré avec la fuite de documents sensibles. La direction de la sûreté a été réformée et le département de la protection de l'information a été créé.

Dans cette entreprise, le risque informationnel est perçu comme étant global : de la perte / vol de documents au RGPD. La mention d'image / notoriété de l'entreprise reste le dénominateur commun à l'ensemble des risques. M Ronand insiste sur la perméabilité de la menace externe. La diversité des fournisseurs favorise les vulnérabilités. Ils doivent, en effet, pour la plupart, se connecter à un réseau, multipliant ainsi les vulnérabilités. Les mesures de prévention / protection s'organisent selon le schéma de la défense en profondeur : de la sûreté (sécurité périphérique et périmétrique) à la protection des infrastructures réseaux. Selon M Ronand, la blockchain n'est pas une technologie d'avenir en matière de protection de l'information. L'entreprise fonctionne avec un système de bases de données qui répond bien aux enjeux de l'entreprise. Le concept de

zéro trust est dans l'idéal, un bon moyen de se prémunir des menaces. A sa connaissance, seul le GAFAM Google a réussi à appliquer le concept.

M Ronand expliquait qu'un des enjeux majeurs du risque informationnel résidait dans l'Intelligence Artificiel (IA), notamment appliquée aux véhicules autonomes. Bien qu'une technologie d'avenir, la sécurité des véhicules autonomes est difficile à garantir. D'autre part, l'IA a besoin d'être alimentée en connaissances. Les véhicules doivent communiquer entre eux pour que l'IA soit opérationnelle (machine learning). Cet échange de flux de données pose un problème quant à la sécurité (confidentialité, intégrité et disponibilité) des communications.

Le premier problème est de nature juridique, quid de la responsabilité en cas d'accident, conducteur ou IA ? Tesla a réglé le problème en indiquant que le conducteur devait toujours avoir les mains sur le volant, la responsabilité par la même occasion.

La culture et la politique urbaine de la ville posent également un problème en matière de sécurité.

Certains pays comme les États-Unis observent une discipline stricte dans le Code de la route ; tandis que d'autres, comme l'Iran, n'observent aucune règle en la matière. Il prenait l'exemple qu'une voiture passe au vert, mais également au rouge. Ce qui pose un problème pour l'IA qui n'a pas la capacité de décider si oui ou non il faut marquer l'arrêt.

La politique urbaine joue aussi un rôle en matière de sécurité. Les États-Unis disposent d'un réseau structuré, quadrillé, carré (1re avenue, 2e avenue, etc.). Cette disposition facilite le travail de l'IA, car elle peut modéliser des équations mathématiques fiables et ainsi prendre plus facilement des décisions. De même, la modélisation de l'IA sur une autoroute est bien plus simple (signalisation quasi absente, ligne droite, vitesse des véhicules, etc.).

Les forces de l'ordre exprimaient le besoin de stopper le moteur des véhicules à distance, ce qui est possible par la technologie des voitures autonomes. Toutefois, selon M. Ronand, la sécurité n'est pas 100 % garantie (tout système est portable). En ce sens, les moteurs des véhicules des forces de l'ordre pourraient être également stoppés en cas de course poursuite. Mais également, des groupes terroristes pourraient pirater le système d'un fourgon blindé, le jetant sur une foule, ou bien stopper quelques voitures sur l'autoroute provoquant un carambolage mortel.

Enfin, l'IA peut être facilement trompée. Des tests ont montré que le fait de coller des autocollants sur des panneaux de signalisation suffisait à fausser l'interprétation de l'IA. Pour appuyer ce propos, M. Ronand nous a partagé un RETEX. Une personne avait acheté plusieurs téléphones (GPS activés), connectés à l'application Waze, qu'ils avaient mis dans une brouette, dans l'objectif était de simuler un embouteillage. Ce système a suffi à tromper l'application Waze.

Afin de pallier tous ces risques, l'entreprise dispose d'un service dédié à l'analyse des vulnérabilités et des modes opératoires envisageables, pour contrer toute tentative de malveillance.

Pour conclure, l'expert nous a partagé un retour d'expérience, sur le cas d'une cyberattaque, en l'occurrence le cryptolocker wannacry. Le ransomware a paralysé le système de production du groupe qui a dû stopper les activités. Il a exploité en parallèle l'exploitation d'une pièce jointe piégée par mail et une faille SMP d'un partage de fichier. La politique de l'entreprise a été de ne pas payer la rançon. Le nettoyage a consisté à réinstaller toutes les machines, la mise à jour des Firewall. L'analyse a permis d'identifier trois patients zéro, mais les équipes n'ont pas réussi à isoler le premier patient zéro.

Interview d'un dirigeant d'une PME de transport routier

En tant que dirigeant d'un PME de transport routier (location de chauffeurs) , pensez-vous qu'une atteinte à vos données (accès, intégrité etc.) pourrait conduire à un arrêt total de votre activité ?

- Compromission des données peu impactante
- Cloisonnement des systèmes d'information des entreprises pour lesquelles nous sous-traitons
- Stockage sur leurs systèmes, ils gèrent les SI
- Informations accessibles via plusieurs appareils

Avez-vous été sensibilisé, formé à ces risques ?

- Non, nous avons simplement signé une charte informatique donnée par les clients.

Quels sont les risques informationnels spécifiquement liés à votre secteur d'activité ?

- Accès à la grille tarifaire
- Peu de concurrence dans ma région, risque limité

Lors de l'achat d'un équipement informatique ou électronique, considérez-vous les normes de cybersécurité comme un élément à prendre en considération ?

- Oui, dans une certaine mesure.

Prenez-vous des mesures afin de garantir la protection de l'information au sein de votre entreprise ?

- Oui, nous avons notamment une déchiqueteuse afin de s'assurer de la bonne destruction des supports
- Matériel de vidéosurveillance à venir

Quelle part approximative de votre budget cela représente-t-il selon vous ?

- Faible mais proportionnée aux risques

Quelle a été l'évolution de ces mesures de protection au fur et à mesure de votre développement ?

- Au début absence de matériel
- Accroissement des mesures de protection au fur et à mesure du développement

Dans le cas où vous développeriez votre activité, pensez-vous que votre entreprise serait plus exposée aux risques informationnels ? Prendriez-vous des mesures particulières ?

- Oui, développer notre système de vidéo surveillance

Vis-à-vis de la crise, avez-vous été impacté ?

- Oui, positivement

Aviez-vous un PCA ?

- Non

Allez-vous en mettre un en place ?

- N’ayant pas été impacté négativement par la crise, je ne prévois pas cela pour le moment

Interview d'un responsable logistique chez un grand groupe de la distribution sélective.

Quels sont les réseaux de transport exploités par votre société ? Routier, maritime, ferroviaire.

- Les trois sont utilisés.
- La plupart des groupes de la société utilisent la route et l'aérien.
- Le maritime et le rail sont moins développés mais sont toujours opérationnels.
- Globalement, avec la crise covid-19, les transports aériens ont perdu du volume de transport de l'ordre de x2 – x10.
- Les modes de transports dépendent des conditions extérieures : urgence, coût, espace demandé. Une entreprise choisit son mode de transport en fonction du besoin de rapidité, du type de marchandise et d'un calcul de coûts vis-à-vis du transport.
- Dans une industrie, il y a en général un schéma de transport de base et un schéma en mode dégradé.

Qu'est-ce qui est internalisé / externalisé dans votre supply chain ?

- Les moyens de transport sont externalisés par tout le monde (avions, bâteaux, etc.), et l'activité est donc donnée à une entreprise tierce.
- Les chargeurs détiennent rarement ces moyens.
- On peut externaliser des systèmes d'informations et l'organisation du cycle de transport. IKEA est un cas particulier qui a internalisé totalement la supply chain grâce à leur TMS home made (remplacé depuis par Oracle).

Avez-vous des entrepôts en propre ou confiez-vous ces tâches à des prestataires ?

- Très externalisé, c'est un business d'assets pour sociétés spécialisées. (Bâtiments, terrains, etc.)
- IKEA est encore une fois à l'opposé de la tendance générale : ils ont des terrains, des manutentionnaires, etc. Ikea a par ailleurs ouvert des entrepôts gigantesques dans une friche industrielle à Valles en Espagne, dépassant largement les tailles moyennes d'entrepôts (<50 000 m²).
- La culture de la logistique est intimement liée à celle de l'entreprise, centralisée ou décentralisée.
- L'internalisation de la logistique dépend aussi du cœur de métier et du type d'activité.

Comment tracez-vous vos produits ?

- Il existe énormément de solutions sur le marché avec différents canaux. La solution adoptée dépend simplement de la pertinence de l'information. Wakeo et AirLiquide ont fait un travail intéressant sur le sujet.
- Il existe des business cases mais la traçabilité n'est pas une exigence et n'est pas systématique. Elle dépend beaucoup de la logistique et du besoin logistique du chargeur.

-Y a-t-il des risques informationnels pour votre groupe au niveau supply chain ?

- Oui, il y a beaucoup de risques informationnels, notamment au niveau des ports (Rotterdam par exemple).
- Des acteurs se sont spécialisés sur le sujet, comme Lars Jensen sur LinkedIn, fondateur de Sea Intel. Il produit du conseil pour des armateurs, banques d'affaires, chargeurs, etc. Il suit les questions de cybersécurité liées aux problématiques de conteneurs. On peut avoir accès à des fonctionnalités du navire, à son contenu, etc. Le port est aussi à risque. Il est possible de savoir d'où le concurrent expédie, ce qu'il y a dans son conteneur, etc.
- En fait, tout ce qui rentre dans le TMS est à risque mais le risque est le même que pour n'importe quelle solution du cloud.

Voyez-vous des conséquences pécuniaires directes provenant de risques informationnels ?

- Difficile d'exploiter cette information pour nuire à l'entreprise.
- Un des moyens les plus efficaces pour atteindre économiquement une entreprise reste d'attaquer la supply chain, à l'exemple de NotPetya chez Maersk

Etes-vous familier avec la notion de blockchain dans le secteur des transports ? Est-ce une technologie que vous utilisez au sein de votre entreprise ?

- Des projets sont à l'étude, mais plus sur la lutte contre la contrefaçon que sur le transport.

Mot de conclusion : Les SI se multiplient pour faire fonctionner les supply chains, de plus en plus comlpexes. Quelqu'un de mal intentionné peut aisément déstabiliser une entreprise industrielle via sa supply chain et ses portes d'entrées numériques.

Sources

« France Logistique 2025 », Ministère de la Transition écologique et solidaire, 29/09/2019.

« Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs des dit secteurs », Legifrance.

« Le transport ferroviaire en France – Faits et chiffres », Statista Research Department, 17/03/2020
https://fr.statista.com/themes/2754/le-transport-ferroviaire-en-france/#dossierSummary__chapter1
« Transport ferroviaire de marchandises », Ministère de la Transition écologique et solidaire, 12/11/2018
https://www.statistiques.developpement-durable.gouv.fr/transport-ferroviaire-de-marchandises
https://www.geoportail.gouv.fr/carte

Fédération des industries ferroviaires

Francis Dudzinski, « *Le chinois MA Steel reprend Valdunes* » Usinenouvelle.com, 02/06/2014.
Liste des entreprises de transport de marchandises par département, Chauffeur Poids Lourd, 2018

Laurent Lagneau, « Le parc de véhicules P4 de l'armée de Terre fond à vue d'œil », Opex 360, 03/03/2013
http://www.opex360.com/2016/03/03/le-parc-de-vehicules-p4-de-larmee-de-terre-fond-vue-doeil/
« Defender : le véhicule polyvalent de l'armée de Terre », Ministère des Armées, 28/06/2010.

D. L., « Quand l'armée française préfère rouler américain », BFM Business, 04/05/2015.

Laurent Lagneau, « Le ministère de la Défense a commandé 520 véhicules pour l'opération Sentinelle », Opex 360, 10/02/2016

Laurent Lagneau, « L'armée de Terre a reçu 150 motos Yamaha XTZ 660 Ténéré », Opex 360, 17/04/2015

« Les chiffres clés de la Défense 2019 », Ministère des Armées, 28/08/2019.

« Les chiffres clés de la Défense 2018 », Ministère des Armées, 11/09/2018.

Laurent Lagneau, « Nexter a livré le dernier Engin Blindé du Génie-VALorisé à l'armée de Terre », Opex 360, 05/02/2014.

« PTA 2 » Military Today.

« Véhicules », Ministère des Armées.

« Les chiffres du transport fluvial et maritime 2019 » Clic & Sea, 2019.

« Liste des navires de la Marine nationale (France) », Wikipedia.

« La France acteur maritime du 21e siècle », Direction des affaires maritimes, 2019, en ligne

« Flotte », CMA-CGM.
« Le transport de passagers : ferries et navires rapides », Armateurs de France, en ligne

Vincent CALABRESE « La croisière, un marché qui continue de croître », L'antenne, 26/09/2018.

Christophe ALIX, « *Livraison par drones : Amazon ouvre un centre de R&D à Clichy-la-Garenne* », Libération, 18 mai 2017.

Emmanuelle FORTUNE, Mickaël CHION, « Focus déposants de brevets à l'INPI en 2018 », Observatoire de la propriété intellectuelle de l'INPI, Décembre 2019.

L'Expansion l'Express, « Le Dieselgate, scandale automobile de triche généralisée aux contrôles pollution ».

Nolwenn COSSON et Adeline DABOVAL, « *Fermeture des entrepôts Amazon : les coulisses d'une décision radicale* », Le Parisien, 15/04/2020.

Site de la Commission nationale de l'informatique et des libertés (CNIL), Sanction.

Site de la Commission nationale de l'informatique et des libertés (CNIL), « *Les dispositifs de géolocalisation GSM/GPS* », 15/06/2009.

Site de la Commission nationale de l'informatique et des libertés (CNIL), « *L'analyse d'impact relative à la protection des données (AIPD)* ».

Ayoub FANDI, « Cybersécurité et culture d'entreprise », Les Echos, 13/02/2019

D, Palmer. « Ransomware : la principale leçon de Maersk dans son combat contre NotPetya », ZDNET, 03 /03/2020.

Organisation Maritime Internationale.

Dr Marco Balduzzi, « AIS ExposedUnderstanding Vulnerabilities & Attacks 2.0 », Blackhat;

L, Kellion. « Ship hack 'risks chaos in English Channel », BBC, 7/06/2018.

« Code of Practice Cyber Security for Ships », Department of transport, 2017.

« Rapid growth in cyber-attacks on smart mobility 2010-2019 », upstream, 19/05/2020.

ISO/TR 14813-1, IS0, 2015.

K, Hyatt. « New study shows just how bad vehicle hacking has gotten », Cnet, 18/12/2019.

G, Ryckmans. « Google Maps: un artiste provoque un embouteillage virtuel en se promenant avec 99 smartphones », RTBF, 4/02/2020

J, Carter. « Hacked Driverless Cars Could Cause Collisions And Gridlock In Cities, Say Researchers », Forbes, 5/03/2019

A, Drozhzhin. « Can you hack a train? », Kaspersky, 29/12/2015.

K, Hall, « Hacking train Wi-Fi may expose passenger data and control systems », The Register, 11/05/2018

« Revue stratégique de Cyberdéfense », SGDSN, 12/02/2018

« Sensibilisation et initiation à la cybersécurité », CyberEdu, 05/11/2015.

Renaud CHASLE, « Digitalisation du TRM : Où en est-on vraiment ? », Transport Info, 11/02/2019.

« Microsoft s'intéresse au suivi de camions en temps réel », Actu Transport Logistique, 22 mai 2018, en ligne.

« Logistics and Fleet Management », Microsoft.

« Utiliser la blockchain dans sa chaîne logistique », Agro Media, 09/04/2020

Fiche ORACLE OTM, Supply Chain Magazine, 2014

Les Cahiers de l'Observatoire n° 178, Décembre 2001.

Oliver WYMAN, « Time For Transportation & Logistics To Up Its Cybersecurity As Hackers Put It On Target List », Forbes, 28/06/2017.

« Ferroviaire : objectif cybersécurité », FIEEC, 17/09/2020

« Une coopération renforcée entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Établissement public de sécurité ferroviaire (EPSF) », ANSSI, 20/03/2018, en ligne https://www.ssi.gouv.fr/publication/une-cooperation-renforcee-entre-lanssi-et-lepsf/

Sylvain ARNULF, « Connecter 160 millions de pneus par an à l'horizon 2024, l'objectif (ambitieux) de Michelin », L'Usine Nouvelle, 27/11/2019, en ligne

« L'IoT, une source complémentaire de données au service des opérations chez SNCF », # DigitalSNCF, 12/10/2018.

Marie-Eve DECROOCQ-DUMAYET « Comment l'Internet des Objets améliore la gestion des transports urbains ? », CGI, 13/09/2016, en ligne.

« The Internet of Things in Transportation », Alcatel Lucent.

Harriet TAYLOR, « Metro transport systems eyed after hack attack in San Francisco », CNBC, 28/11/2016.

Dirk NEUBAUER « Düsseldorf zwischen Update und Absturz: Schwarzer Donnerstag bei der Rheinbahn - Tausende kamen zu spät », Report-D, 20/04/2017;

Chris GRAHAM, « Cyber-attack hits German train stations as hackers target Deutsche Bahn », The Telegraph, 13/05/2017.

John BELTZ SNYDER « Researchers hack a self-driving car by putting stickers on street signs », Autoblog, 4/08/2017.

Olivia SOLON, « Team of hackers take remote control of Tesla Model S from 12 miles away », The Guardian, 20/09/2016.

Elizabeth WEISE, « Chinese group hacks a Tesla for the second year in a row », USA Today, 15/12/2019.

V. Saraogi, « UNCTAD analyses impact of US-China trade war on shipping », Octobre 2019.

C. J. McMahon, « Maritime Trade Warfare, Navar War College Review », volume 70, 2017.

A, Biazetti, « 5 key points about TradeLens platform security », Septembre 201.9

H-M. Thomas, « Le transport maritime face aux nouveaux risques », L'argus de l'assurance, 2015.

M. Untersinger, Le virus Petya a coûté plus d'un milliard d'euros aux entreprises, Le Monde, 07/11/2017.

S. Ciemcioch, « 3PL vs 4PL Logistics : Best Definition, Explanation and comparison », Warehouse Anywhere, Aout 2018.

A.Pradi, « Ports and terminals: the missing element for full optimization », Tradelens, 2020.

S. Singh, « GPS Tracking Device Market worth $3.7 billion by 2025 », Markets and Markets.

N. Guibert, « La nouvelle guerre du GPS et ses risques », Le Monde, 02/05/2019.

« Qu'est-ce que la blockchain », Blockchain France.

David Parkins, « The great chain of being sure about things », The Economist, 31/08/2015.

Loïc Le Gurun, « Blockchain et sécurisation des données », Force Plus, 28/06/2018.

Joëlle Toledano, « Les enjeux de la blockchain », France Stratégie, juin 2018.

Samir Azizi, « La technologie blockchain au service du transport de conteneurs maritime ? » Transport Shaker - Wawestone, 17/05/2018.

« Blockchain, logistique et supply chain : panorama des possibilités », Blockchain France, 23/08/2017.

« Resolving the Blockchain Paradox in Transportation and Logistics », Boston Consulting Group, 29/01/2019

« La blockchain dans la logistique, BITO Systèmes ».

« Renault Chasle, Informatique transport : Qu'est-ce que la BlockChain ? », Transport Info, 25/06/2018.

« Présentation de Tradelens », Tradelens, 17/04/2019.

Mourad Krim, « Blockchain, les entreprises de transport et de logistique doivent intensifier leur collaboration », IT Social, 31/01/2019.

A.Descamps, « Allianz : Une décennie de risques maritimes analysés », Journal de la Marine Marchande, 05/06/2019.