Sûreté, sécurité et résilience des réseaux de transport à l'âge du numérique et des menaces hybrides

Par **Antoine-Tristan MOCILNIKAR**
Ministère de la Transition écologique et solidaire
Ministère de la Cohésion des territoires
et des Relations avec les collectivités territoriales

Interactions entre les transports, les territoires, la sûreté et la sécurité

La question du transport s'inscrit dans un contexte de libéralisation et de foisonnement technologique. C'est dans ce cadre renouvelé que nous affrontons les questions de sûreté et de sécurité. Le transport, sous certains de ses volets, est dans la complétude de la logique libérale et progresse dans cette voie pour la plupart des autres. La libéralisation du transport routier de fret au niveau européen est déjà ancienne, suivie par l'accroissement de la concurrence dans le domaine du rail grâce aux réformes, en France et dans l'Union. La concurrence au taxi est apparue récemment. Les bus, eux, n'auront été libéralisés complètement qu'il y a quelques années. Nous sommes donc dans un contexte de décentralisation, schumpétérien et libéral.

Les interactions entre le monde du transport, les domaines de la sécurité et de la sûreté, et l'action collective au niveau des territoires, dessinent un champ complexe. Des événements majeurs touchant la sûreté et la sécurité des transports ont de surcroît renouvelé la problématique :

Inondation de l'Autoroute A10 le 5 juin 2016 dans le département du Loiret.

Du 31 mai au 10 juin 2016, un phénomène climatique inédit a induit la fermeture de l'autoroute A10 au nord-ouest d'Orléans, infrastructure majeure et stratégique du réseau français. Des précipitations totalement exceptionnelles se sont traduites par de très importantes stagnations qui se sont rapidement étendues, entraînant la submersion complète de l'autoroute en quatre points sur un tronçon de plusieurs kilomètres, avec des hauteurs d'eau allant jusqu'à 1,40 mètre au-dessus de la chaussée. Plusieurs centaines de véhicules se sont trouvés bloqués entre les zones noyées, ce qui a nécessité la mobilisation du gestionnaire mais aussi de l'armée, pour évacuer près de trois cent cinquante usagers, puis pour les loger et les accompagner. Lors de cette crise, il n'était pas certain que l'autoroute puisse être récupérée. Le concessionnaire a engagé des travaux importants.

L'incendie du poste RTE à Montparnasse a impacté, en juillet 2018, le trafic de la gare pendant une semaine. Cela a mis en lumière la liaison entre énergie et transport dans une logique de sécurité globale. Les investissements à mobiliser pour éliminer, partout en France, ces potentiels effets domino sur des infrastructures essentielles sont importants.

En septembre 2018, l'écroulement du pont de Gênes en Italie a, lui, rappelé que les lourds investissements d'entretien deviennent très difficiles à assumer pour nos sociétés. De manière moins catastrophique, les résultats des audits concernant le réseau routier national non concédé, réalisés par les bureaux d'études Nibuxs et IMDM et publiés en juillet 2018 par le ministère de la Transition écologique et solidaire, sont préoccupants. Ils indiquent que 17 % des routes et 7 % des ponts sont gravement endommagés et nécessitent des réparations structurelles, que 30 % du parc d'ouvrages nécessite un entretien ou de grosses réparations. Avec un budget équivalent à l'effort budgétaire des dix dernières années, en 2037, 62 % des chaussées seraient très dégradées (29 % en 2017) et 6 % des ponts seraient « hors service ». Si l'on continue à dépenser ce montant annuel effectif de 666 millions d'euros jusqu'en 2022, il faudra ensuite investir 1,3 milliard d'euros par an jusqu'en 2037 pour revenir à l'état actuel. Une étude conjointe entre le CEREMA et Carbone 4 (2018) a d'ailleurs montré le lien entre infrastructures et changement climatique, notamment l'impact de celui-ci sur elles.

À partir de novembre 2018, des « Gilets jaunes » se sont greffés sur les réseaux linéaires de transport. Ils les ont bloqués en de nombreux points et ont monté des barrages filtrants particulièrement pénalisants pour le transport de fret. Des membres de ce mouvement ont pris d'assaut des péages autoroutiers et les ont parfois détruits. Ils ont également détruit une gendarmerie routière, un centre de supervision urbaine et des plateformes logistiques. Des manifestants ont mis en danger des ponts, ou encore, ont fait de brèves incursions dans les gares et sur les lignes de chemin de fer. Certains ont pu vouloir manipuler les informations.

Félicitons les trois héros américains qui ont déjoué l'attentat perpétré par l'État islamique dans le Thalys n°9364 reliant Amsterdam à Paris, le 21 août 2015. Et ayons une pensée pour Mauranne et Laura, assassinées le dimanche 1er octobre 2017 en gare de Marseille Saint-Charles, dans un attentat revendiquée par l'État islamique.

La résilience, qui part de la gestion de crise, des catastrophes et des réactions immédiates, peut apporter une méthodologie pour affronter ces sujets. Toutefois, dans son concept global, au sens de la Fondation Rockefeller (1), elle prend toutes les temporalités, y compris celle de l'aménagement de très long terme. Partons de la dynamique issue de la révolution digitale, puis intégrons les questions de sécurité et de sûreté pour finalement définir la boîte à outils que la résilience nous propose.

(1) Le projet *100 Resilient Cities*, lancé en 2013 par la fondation Rockefeller, vise à créer un réseau de « villes résilientes », « plus résistantes aux stress d'ordres physique, social et économique ».

Numérisation et mobilisation des données

Ce numéro des *Annales des Mines* montre que l'usage des données, des systèmes d'information et des plateformes numériques transforme radicalement le domaine du transport. Les vecteurs et les contenants de transport, tout comme les usages, se numérisent. Les systèmes communiquent entre eux et avec le reste du monde. La dématérialisation des échanges documentaires, de la transmission des ordres et des informations, s'ajoute à la généralisation du numérique sur les terminaux (manutention) et à bord des vecteurs de transport.

L'usage d'une multitude de données permet l'amélioration de la pertinence, une plus grande complétude de la prise de contrôle ainsi que le renforcement de la confiance. L'agilité associée à un aplatissement des organisations accroît l'efficacité. Une voiture particulière n'est utilisée que 1 % du temps. Le numérique permettra de se tourner vers la « servicisation » de l'automobile. Les infrastructures sont elles aussi sous-utilisées. Leur potentiel maximum *(peakload)* n'est atteint que 3 % du temps. Des camions continuent à circuler à vide ; d'autres attendent des journées entières devant des guichets administratifs ou douaniers...

Il est donc logique que les gains d'efficacité potentiels liés au numérique dans les transports soient très importants. Pour McKinsey (2013), un meilleur usage numérique des données permet de créer de 720 à 920 milliards de dollars de valeur par an au niveau mondial, dans le seul domaine du transport. Une bonne gestion du transport est également un point-clé pour la maîtrise du changement climatique. Avec un quart des émissions de CO_2 émis dans le monde, le transport est le deuxième émetteur de gaz à effet de serre, derrière la production d'énergie et d'électricité.

La mobilisation des données et l'utilisation accrue de l'intelligence artificielle ne vont qu'accentuer la vélocité du traitement de l'information, ce qui permet d'accroître nos capacités à révéler les éléments-clés du domaine du transport à tous les horizons, de prédire les évolutions ainsi que d'être capables de réagir et de décider de manière réfléchie en fonction d'objectifs prédéfinis.

Plus précisément, le champ des domaines concernés est très large :

- optimisation de la taille, du mix et du partage des réseaux ;
- gestion de l'offre et de la demande ;
- optimisation de la maintenance et de son calendrier ;
- tarification des congestions ;
- optimisation de la composition des flottes ;
- amélioration de l'approvisionnement et de son efficacité ;
- rapports et aide à la décision ;
- prévention des accidents ;
- évaluation des meilleures pratiques ;
- conception de la valeur ;
- sobriété de la construction ;
- mise en œuvre et stratégie ;
- optimisation de la technologie ;
- décisions de déploiement ;
- optimisation de la main-d'œuvre et du recrutement ;
- allocation du capital fondé sur le risque ;
- optimisation du déploiement de réseaux intelligents ;
- sélection optimisée de l'efficacité énergétique, ordonnancement ;
- achats et gestion des stocks ;
- planification des opérations.

La révolution des gains d'opportunité permet une meilleure synchronisation des offres et des demandes dans tous les domaines. Cela concerne aussi bien des sujets de très court terme comme la congestion, que de moyen terme comme la programmation de flotte, ou de très long terme comme le choix d'infrastructure ou même de filière industrielle.

Comme dans les autres secteurs économiques, la numérisation du transport fait peser de nouveaux risques sur cette activité et ses acteurs. L'ensemble des systèmes d'information constituent de potentielles portes d'entrée, exploitables par des pirates informatiques, et qu'il convient donc de sécuriser. En juin 2017, le groupe numéro un mondial du *shipping,* Maersk, a subi l'une des premières cyberattaques d'envergure dans ce secteur. Il a vu les réservations sur certains de ses plus grands terminaux portuaires (Rotterdam, New York, Mumbai) bloquées plusieurs heures durant par un logiciel de rançon *(ransomware)*. Le vol de marchandises et la prise de contrôle de vecteurs de transport font aussi partie des menaces prises de plus en plus au sérieux. Des *hackers* ont, ainsi, réussi localement à détourner le flux de données de capteurs de véhicules intelligents insuffisamment cryptés.

À l'heure des menaces hydrides, sûreté et sécurité se décloisonnent et tendent vers une sécurité globale

La sûreté des transports comprend l'ensemble des actions entreprises pour assurer la protection du patrimoine des opérateurs – qu'il relève des infrastructures ou des moyens de transport eux-mêmes –, mais aussi de leur personnel et des marchandises transportées contre les actes illicites (violences, vols, déprédations, ainsi que l'utilisation abusive de la chaîne logistique pour le transport frauduleux de matières, d'équipements ou d'êtres humains). C'est un travail qui concerne les opérateurs et, plus largement, toutes les parties prenantes. Il s'agit aussi bien de l'État que des collectivités locales, des clients et des usagers, entreprises et individus. La sécurité est, quant à elle, relative aux dysfonctionnements techniques sans causes anthropiques volontaires.

Le monde de la menace lui-même évolue. Les menaces deviennent hydrides dès lors que sont exploitées des synergies entre divers acteurs et diverses activités. Ces menaces sont nombreuses et en constante évolution : les outils utilisés vont des faux profils sur les médias sociaux à l'espionnage et à la désinformation, de la manipulation aux tentatives d'escroquerie, des cyberattaques sophistiquées jusqu'à l'emploi manifeste de la force, en passant par tout l'éventail des actions intermédiaires. Les outils d'influence hybrides peuvent être utilisés séparément ou de manière combinée, selon la nature de la cible et le résultat souhaité. En réponse, la lutte contre les menaces hybrides doit elle aussi être dynamique et adaptative pour rester en phase avec les déclinaisons des activités d'influence hybrides et anticiper des attaques ultérieures, en déterminant de nouveaux moyens de défense.

En pratique, pour traiter de ces problèmes de sécurité, et sur la base du code de la défense et de la loi de programmation militaire, l'administration a produit, avec les opérateurs, un nombre considérable de textes. C'est notamment la documentation liée au Secteur d'Activité d'Importance Vitale (SAIV) qui s'applique aux transports. S'y ajoute la notion nouvelle, datant de 2018, d'Opérateurs de services essentiels (OSE), elle-même liée à la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS ». Des dispositions concernant le secteur des transports sont également incluses dans le plan Vigipirate ainsi que dans les Plans « Pirate » d'intervention adaptés chacun à un type de risque particulier : plans Pirate Mobilités terrestres, NRBC (nucléaire, radiologique, biologique ou chimique) ou Piranet (crise d'origine informatique)... Ces éléments ont une déclinaison territoriale importante.

Sûreté et sécurité correspondent à des problématiques longtemps considérées comme indépendantes. Les disciplines associées ont historiquement évolué de façon séparée. En sûreté

comme en sécurité, la notion de *risque* joue un rôle fondamental. En revanche, l'évaluation de la menace est radicalement différente selon sa nature malveillante ou accidentelle. Dans le premier cas, l'origine des menaces à évaluer est par définition hors de tout contrôle de l'analyste et couvre un champ des possibles extrêmement vaste. Dans le second cas, les caractéristiques des dangers sont plus accessibles, et le nombre de scénarios à considérer peut généralement être réduit à un ensemble restreint mais suffisant pour être considéré comme significatif. En sûreté, la menace est potentiellement intelligente et adaptative. Elle peut tenir compte des vulnérabilités du système considéré, voire des contre-mesures et des réactions d'ordre défensif, alors que menaces et vulnérabilités n'ont pas d'interactions dynamiques en sécurité.

Dans le même ordre d'idées, une fois les dangers identifiés en sécurité, ils sont souvent considérés comme relativement stables dans le temps, faisant de l'utilisation de scénarios de référence une approche adaptée ; dans le cas de la sûreté, les profils, les motivations et les moyens des attaquants évoluent plus rapidement et de façon moins prévisible, car ils dépendent de nombreux facteurs. La logique de « course » entre attaquants et défenseurs contribue aussi à l'instabilité et à la dynamique de ces facteurs. Les référentiels doivent être mis à jour beaucoup plus fréquemment.

Différentes, sécurité et sûreté partagent en fait de substantiels points communs qui, progressivement identifiés, ont déjà permis diverses inspirations réciproques, aussi bien d'un point de vue méthodologique que technologique ou architectural. Ainsi, la technique des arbres de défaillances ou l'approche de défense en profondeur, amenant à combiner plusieurs types de contre-mesures complémentaires et indépendantes, fonctionnent autant en sûreté qu'en sécurité.

Si elles demeurent différentes, sûreté et sécurité doivent impérativement converger : la séparation pouvait encore faire sens quand l'objet de leur préoccupation était séparé, mais tel n'est plus le cas. Lorsque les exigences et les mesures de sécurité et de sûreté s'appliquent sur les mêmes systèmes, les risques d'antagonismes sont réels. Un exemple simple permet d'illustrer ce dernier cas de figure : un système de fermeture de porte automatisé pourra ainsi être conçu pour laisser la porte ouverte en cas de panne selon des exigences de sécurité. Il sera conçu pour verrouiller les portes dans le même cas en suivant des exigences de sûreté. Au minimum, si la convergence ne peut être complète, il devient impératif de mieux caractériser et modéliser leurs interdépendances. La maîtrise de tous les risques pesant sur le transport, mais aussi l'optimisation des ressources en conception et en exploitation qui y sont consacrées, en dépendent. Sûreté et sécurité tendent vers une sécurité globale.

Bâtir une stratégie de sûreté et de sécurité autour de la notion de résilience

Une stratégie de résilience prend en compte tous les risques : le risque économique, la difficile utilisation des infrastructures en raison de la congestion, le risque lié au climat, à la pollution et au bruit. Il ne faut pas oublier les risques physiques, liés à la malveillance, au terrorisme, et aux États étrangers hostiles, en plus des risques sociaux, de gouvernance, et politiques. Le risque technique, s'il est bien sûr toujours présent, n'est désormais plus le seul qui doit être analysé. Ces questions de résilience sont là pour le planning de long terme et pour la gestion de crise. Quand il y a des inondations, il faut évacuer des gens ; quand des risques technologiques se matérialisent, il faut aussi évacuer des gens. Donc, le transport doit participer à la résilience. Tous les territoires doivent être impliqués : il n'y a pas un territoire plus important qu'un autre, il faut au contraire les enchâsser. L'individu, le consommateur, le citoyen, l'étudiant, le professeur sont les grands acteurs de la gouvernance de ces sujets et c'est cette gouvernance qui fait la résilience.

Dans nos administrations, la résilience a été définie dans le *Livre blanc sur la Défense* de juin 2008 comme la volonté et la capacité à résister aux conséquences d'une agression ou d'une catastrophe

majeure, puis à rétablir rapidement la capacité des institutions, de la société et de la vie économique, à fonctionner normalement, ou à tout le moins dans un mode socialement acceptable.

La résilience renvoie au systémique, par opposition au sectoriel, et doit se concevoir à l'échelle globale en raison des interdépendances, notamment des réseaux qui supportent nos sociétés. Dans cette logique, nous avons déjà une expérience longue, depuis la fin des années 1970. Citons comme exemple la sécurité routière. Dans une approche systémique, il n'y a pas que l'automobiliste qui est responsable, il y a ceux qui ont fait la route, la voiture, la réglementation… : chacun contribue à l'insécurité routière. À partir de 1972, le mode de gestion de cette sécurité routière a profondément évolué dans notre pays. Une meilleure coordination des entités chargées de ce thème dans les différents ministères (Intérieur, Transports, Équipement et Travaux publics, Enseignement) est mise en place. Une batterie de mesures accompagne ce mouvement, démarrant du continuum éducatif mis en place de l'école primaire au collège, complété, avec le permis à points, par des stages de sensibilisation pour les conducteurs contrevenants. S'ajoutent à cela des mesures d'amélioration des infrastructures, de limitation des vitesses, de meilleure signalisation et de répression, mais aussi d'élévation de la sécurité pour les voitures et les passagers.

Le premier point structurant est donc celui de la temporalité. Le lien entre infrastructure et usage s'inscrit dans une logique de résilience. Dans l'histoire de l'aménagement des pays, les stratégies pour les infrastructures et leur usage ont mis du temps à être définies simultanément. Le temps a permis de réaliser la nécessité d'avoir une vision d'ensemble, territorialisée et géographisée. À court et moyen termes, la construction d'infrastructures sera toujours d'actualité mais beaucoup plus lente. Autrement dit, d'un côté la temporalité de l'accroissement des infrastructures est et sera lente, et de l'autre, la temporalité de l'usage est et sera exponentielle. Les trottinettes électriques, les véhicules autonomes, les taxis volants et surtout les plateformes de partage constituent des ruptures essentielles. Ces différents instruments impliquent une importante dynamique dans l'exploitation des infrastructures. Les logiques de résilience de court, moyen et long termes reviennent à confronter ces deux temporalités.

Le pivot temporel de la résilience elle-même est la gestion de crise, avec d'abord le traitement des catastrophes et la mise en œuvre des réactions immédiates, puis la reprise d'activité, la dynamique de post-crise et la reconstruction. En amont, nous avons toujours la normalisation, la certification, la prévention, la préparation et la veille. Ces questions de résilience sont là pour le planning de long terme et pour la gestion de crise.

Le deuxième point est l'aspect territorial. Dans la logique de résilience, la notion d'interconnexion est essentielle. Le territoire rural s'étudie en interconnexion avec la métropole et inversement dans le phénomène métropolitain. Les territoires et la décentralisation ont également leur historicité. Les territoires connaissent une évolution forte de gouvernance depuis quarante ans. Il faut souligner l'accentuation récente de la décentralisation dans le domaine du transport. Des transformations majeures sont encore possibles au demeurant.

Les priorités sont alors d'identifier tous les risques, toutes les temporalités et d'appréhender la logique territoriale. C'est ce que nous appelons la *sécurité globale des territoires*. Ce sont ces éléments qui traduisent la résilience.

Au total, il faut donc renforcer nos capacités d'anticipation et de pilotage des mutations et des adaptations. L'idée est d'optimiser nos transports grâce à une approche intégrée qui prenne en compte simultanément les enjeux économiques, sociaux, financiers, numériques, de sûreté et de sécurité ainsi que les enjeux de gouvernance, à travers une perspective territoriale basée sur un dialogue multipartite œuvrant à anticiper et à suivre les mutations en cours et à venir. Le grand défi est alors de conduire des ensembles, vastes ou plus restreints, en évitant le décrochage. Cela suppose de tenir les performances immédiates, mais plus encore de reformuler les fondamentaux,

de reconstruire des trajectoires de navigation qui puissent faire sens, susciter la cohésion et permettre des réussites collectives.

Bibliographie

CEREMA (2019), *Villes et stratégies de résilience, Enseignements du programme 100 Resilient Cities*, en cours de publication.

CEREMA et Carbone 4 (2018), *Analyse des risques liés aux événements climatiques extrêmes sur les infrastructures et services de transport, note de synthèse méthodologique et exemple d'application*, 3 mai. http://www.carbone4.com/de-plus-vers-resilience-reseaux-de-transport-face-changement-climatique-analyse-de-risque-reseau-de-dir-mediterranee/

GREENBERG A. (2018), "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 31 mai.

McKinsey Global Institute, McKinsey Center for Government & McKinsey Business Technology Office (2013), *Open data: Unlocking innovation and performance with liquid information*, october, Report, McKinsey.

MTES (2018), « Réseau routier national non concédé : résultats d'audits », *Rapport d'audit externe réalisé par les cabinets NIBUXS & IMDM pour le compte du ministère de la Transition écologique et solidaire et du ministère chargé des transports*, 10 juillet.
https://www.ecologique-solidaire.gouv.fr/reseau-routier-national-non-concede-resultats-daudits

Préventique (2019), « Sécurité globale des territoires, restitution des Assises de Lyon », numéro spécial, n°162, janvier.

Premier ministre (2018), *Plan d'action contre le terrorisme*, Dossier de presse, 13 juillet.
https://www.gouvernement.fr/sites/default/files/document/document/2018/07/dossier_de_presse_-_plan_daction_contre_le_terrorisme_-_13.07.2018.pdf

SGDSN (2016), « La sécurité des activités d'importance vitale », SGDSN, 18 mars,
http://www.sgdsn.gouv.fr/communication/la-securite-des-activites-dimportance-vitale/