PRISE EN COMPTE
des enjeux de cybersécurité au sein de la sécurité ferroviaire

Avec la collaboration de

Avant-propos

Cette note a été rédigée dans le cadre d'un groupe de réflexion composé de :

- Laurent CÉBULSKI, directeur général, EPSF
- Sadio BA, coordinateur sectoriel transport, ANSSI
- Thomas CHATELET, responsable projet ERTMS, ERA
- Yseult GARNIER, responsable CyberSécurité Industriel (RCS-I), SNCF RÉSEAU
- Quentin RIVETTE, responsable CyberSécurité Industriel (RCS-I) du Matériel, SNCF VOYAGEURS

Sommaire

Introduction

La généralisation des composants électroniques et des technologies de l'information et la communication, tant au niveau des infrastructures que des matériels roulants (et notamment pour la partie contrôle-commande), fait apparaître au sein du secteur ferroviaire de nouveaux risques pour lesquels la frontière entre ce qui relève de la cybersécurité et ce qui relève de la sécurité de l'exploitation ferroviaire est de plus en plus ténue.

La prise de contrôle totale à distance d'un véhicule automobile par deux chercheurs en 2015 – depuis plusieurs autres démonstrations ont été faites – est une illustration parfaite de l'importance qu'il nous faut accorder à ce risque « cyber » dans le secteur du transport.

Le système ferroviaire a subi, ces dernières années, plusieurs attaques impactant plutôt des systèmes d'information voyageurs ou billettiques. Ainsi, le 29 novembre 2016, un hacker s'est attaqué au système billettique du réseau de transport public de San Francisco pendant *Thanksgiving* (attaque de type « rançongiciel »[1]), rendant l'accès au réseau gratuit pendant plusieurs jours. Plus récemment, le système d'information voyageurs en Allemagne a été altéré, en 2017, par le rançongiciel Wannacry[2].

Entre 2015 et 2016, le réseau ferroviaire anglais a été attaqué quatre fois. Ces attaques ont été évaluées comme étant « exploratoires », mais les pirates informatiques pouvaient accéder à des systèmes de gestion informatiques plus vastes qui contrôlent les signaux[3].

Ces risques « cyber » ne peuvent être dissociés des risques ferroviaires

Ces risques « cyber » ne peuvent être dissociés des risques ferroviaires : la prise de contrôle d'un poste de commande, ayant fait l'objet d'une autorisation de mise en service par l'autorité de sécurité ferroviaire à partir de normes de sûreté de fonctionnement, pourrait avoir des conséquences graves sur la sécurité de l'exploitation. Les normes techniques ferroviaires actuelles ne tiennent quasiment pas compte de la cybermenace. La frontière sécurité ferroviaire / cybersécurité reste à déterminer, aussi bien en matière technique, de périmètre d'intervention et de compétences entre les différentes autorités de sécurité, qu'organisationnel. Il est essentiel de clarifier le fonctionnement à l'interface des deux « mondes » : articulation entre le système de gestion de la sécurité et le système de gestion de la sécurité des systèmes d'information des exploitants ferroviaires concernés.

La connectivité croissante des infrastructures et des matériels roulants entraîne une augmentation importante de leur surface d'attaque. Néanmoins, cette connectivité offre des leviers de performance en matière de supervision ou de mises à jour, mais nécessite d'être parfaitement maîtrisée et cyber-sécurisée par les constructeurs, équipementiers ou exploitants.

La temporalité est un enjeu : le temps « cyber » nécessite des mesures rapides pour appliquer des correctifs aux systèmes (signalisation, maintenance, etc.) afin de pallier toute vulnérabilité, mais le temps de la sécurité ferroviaire impose une analyse de non-régression du système et la garantie que la

[1] Programme malveillant qui chiffre les données présentes sur un ordinateur et demande une rançon en échange de leur déchiffrement.

[2] Rançongiciel ayant impacté de nombreuses entreprises au niveau mondial en 2017

[3] https://www.independent.co.uk/life-style/gadgets-and-tech/uk-rail-network-railways-hacked-four-times-hackers-trains-a7135026.html

mise à jour opérée ne va pas rendre incompatible l'infrastructure avec les matériels roulants qui y circulent, voire dégrader le niveau de sécurité d'exploitation ferroviaire.

Ce document, corédigé par des membres de l'Agence de l'Union européenne pour les chemins de fer (ERA, acronyme anglais), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de l'Établissement public de sécurité ferroviaire (EPSF), de SNCF Voyageurs et de SNCF Réseau, a pour objectifs :

- de rappeler au lecteur les périmètres respectifs des cadres réglementaires ferroviaires et de cybersécurité ;
- de dresser un état des lieux des travaux en cours visant à bâtir un cadre commun entre sécurité et cybersécurité, à renforcer la prise en compte de la dimension cybersécurité dans le domaine ferroviaire et dans les autres modes de transport ;
- de mettre en exergue les sujets (notamment de nature opérationnelle) d'ores et déjà identifiés et qui justifient la nécessité d'un cadre de fonctionnement clair en matière de sécurité « globale » ;
- d'émettre, à ce stade de la réflexion, des recommandations issues des discussions et échanges entre les auteurs de cette note.

Contexte : une menace cyber à prendre en compte dans le transport ferroviaire

Le secteur du transport ferroviaire, entendu ici comme comprenant les gestionnaires d'infrastructure, les entreprises de transport de biens et de personnes, ainsi que leurs prestataires, est un secteur stratégique. Les États se tournent en effet davantage vers le développement de ce moyen de transport pour d'une part, remédier aux nouveaux enjeux de la saturation des réseaux et d'autre part, profiter des avancées technologiques et des nouveaux débouchés économiques et environnementaux apportés par le secteur. L'augmentation constatée du nombre d'acteurs depuis 2006 (43 entreprises ferroviaires et 20 gestionnaires d'infrastructure en France à fin 2018) devrait s'accélérer avec la prochaine ouverture à la concurrence du transport interne de voyageurs. Ce panel d'acteurs très hétérogène (taille des entreprises, trafic, âge et maturité, etc.) impose à la fois un regard global en matière de sécurité et de cybersécurité du système ferroviaire et une vigilance particulière aux multiples interfaces existantes entre l'ensemble des parties prenantes.

Des attaques informatiques à des fins de sabotage, menées par des acteurs offensifs en réponse à des tensions géopolitiques, ont déjà pu être observées à l'international. Ainsi, des tensions géopolitiques entre la France et un autre État ayant des capacités de lutte informatique offensive pourraient provoquer des d'attaques informatiques à des fins de déstabilisation, voire de sabotage, à l'encontre de secteurs stratégiques tels que le transport ferroviaire.

L'ANSSI constate également depuis plusieurs années que le secteur du transport ferroviaire, au niveau mondial, est davantage ciblé par des attaquants aux motivations lucratives. La tendance observée des attaques de type rançongiciel ainsi que les campagnes d'exfiltration de données personnelles à l'encontre des acteurs du secteur devraient se poursuivre. Le secteur du transport ferroviaire français peut être, dès lors, menacé par ces attaques informatiques dont certaines peuvent impacter l'intégrité et la disponibilité des données et les services qu'elles fournissent.

L'ANSSI, ainsi que ses partenaires, observent par ailleurs une évolution dans les activités offensives de certains acteurs allant vers un pré-positionnement[4] au sein des réseaux informatiques de secteurs stratégiques, en France comme dans d'autres pays, sans que l'objectif final de ces compromissions ne soit connu.

Enfin, le secteur du transport ferroviaire connaît, depuis plusieurs années, une numérisation croissante de ses activités et services. Celle-ci impose aux acteurs du secteur toujours plus d'interconnexions de leurs réseaux respectifs augmentant *in fine* la surface d'attaque.

[4] Pré-positionnement : Il s'agit dans ce cas de préparer une attaque massive ou une invasion rapide d'un SI en positionnant des « actifs dormants » qui s'activeront le jour J et qui serviront alors de porte d'entrée.

1. Cadres réglementaires applicables

Selon le champ de compétence dans lequel on se place, les termes employés et les compétences associées sont fondamentalement différents :

- **La sécurité ferroviaire** s'intéresse au fonctionnement global du système, lui-même composé de différents sous-systèmes (infrastructure, matériel roulant, contrôle-commande et signalisation, exploitation, etc.). Les risques sont avant tout techniques et environnementaux.

- **La sûreté de fonctionnement** est l'aptitude de composants (portes, freins, etc.) d'un sous-système à remplir une ou plusieurs fonctions requises dans des conditions données. Elle est utilisée pour établir les démonstrations de sécurité des sous-systèmes techniques.

- **La cybersécurité** est un ensemble de technologies, de processus et de pratiques visant à protéger les réseaux, ordinateurs et données contre les attaques, dommages et accès non-autorisés. Dans un contexte informatique, le terme « sécurité » englobe la cybersécurité et la sécurité physique.

1.1 Le cadre réglementaire ferroviaire

Fortement régulé, le secteur ferroviaire dispose d'autorités de sécurité pour vérifier, par des autorisations et des contrôles, que les acteurs respectent les règles qui s'imposent à eux. En France, c'est l'Établissement public de sécurité ferroviaire (EPSF) qui est l'autorité nationale compétente. Sa création fait suite à la transposition de la directive 2004/49/CE du Parlement européen et du Conseil concernant la sécurité des chemins de fer communautaires qui instaure dans son article premier la création obligatoire, dans chaque État membre, d'une autorité de sécurité ferroviaire.

L'article L2221-1 du Code des transports précise que l'Établissement public de sécurité ferroviaire veille au respect des règles relatives à la sécurité et à l'interopérabilité des transports ferroviaires. Il est l'autorité nationale de sécurité au sens de la directive (UE) 2016/798 du Parlement européen et du Conseil du 11 mai 2016 relative à la sécurité ferroviaire. Il exerce ses missions au sein du système ferroviaire français (les réseaux urbains de métros et tramways relevant de la compétence des préfets).

Sous réserve des missions dévolues à l'Agence de l'Union européenne pour les chemins de fer prévues par le règlement (UE) 2016/796 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour les chemins de fer, l'EPSF est notamment chargé de délivrer les autorisations requises pour l'exercice des activités ferroviaires et d'assurer des activités de surveillance portant en particulier sur les entreprises ferroviaires et les gestionnaires d'infrastructure.

L'établissement public promeut et diffuse les bonnes pratiques en matière de sécurité et d'interopérabilité ferroviaire sur la base de toutes les informations pertinentes disponibles, anime et contribue aux réflexions collectives sur l'amélioration de la sécurité ferroviaire.

Plus précisément, l'EPSF a pour principales missions :

- d'évaluer les demandes d'autorisations nécessaires à l'exercice des activités ferroviaires qui entrent dans son champ : certificats de sécurité uniques d'entreprises ferroviaires, agréments de sécurité de gestionnaires d'infrastructure, autorisations de mise sur le marché de véhicules ferroviaires et les autorisations de mise en service des infrastructures. Il administre le Registre

national d'immatriculation des véhicules, alimente le Registre européen des types de véhicules autorisés et délivre les licences de conducteur de train ;

- de contrôler le respect des conditions de maintien de ces autorisations, moyennant des inspections et des audits sur l'exploitation, l'infrastructure ou l'organisation interne des entreprises. En cas de défaillance, il peut restreindre le champ d'application des autorisations, voire les suspendre ou les retirer ;
- de suivre le niveau de sécurité, en assurant ainsi la classification, la traçabilité et l'analyse des événements de sécurité survenant sur le réseau ;
- d'organiser un retour d'expérience national en liaison avec le secteur et de piloter des actions d'améliorations collectives ;
- d'élaborer et de publier des documents techniques, règles de l'art et recommandations, relatifs à la sécurité ferroviaire, certains textes pouvant avoir valeur de « moyens acceptables de conformité » à la réglementation ;
- d'assister le ministère chargé des Transports dans l'élaboration et l'adaptation des textes nationaux et internationaux (tout particulièrement européens), relatifs à la sécurité et à l'interopérabilité ferroviaire.

La réglementation technique européenne est en premier lieu une réglementation d'interopérabilité. Elle inclut des enjeux de sécurité ferroviaire dans un contexte de libéralisation progressive du secteur qui a débuté par le transport de marchandises en 2006 et qui, dès le début de l'année 2020, se poursuit par celle du transport national de voyageurs.

L'interopérabilité vise à lever, par une harmonisation progressive des règles et des normes, les barrières techniques dressées entre les États au cours de leur histoire. À titre d'exemple, un train souhaitant relier Berlin à Madrid doit encore aujourd'hui être en mesure de circuler sous quatre tensions électriques, six systèmes de signalisation et deux écartements de rails différents. L'harmonisation passe par des travaux longs, lourds et extrêmement coûteux qui ne concernent, à ce jour, que quelques corridors européens dédiés à la grande vitesse et au transport de marchandises entre des installations terminales majeures.

Afin d'accélérer cette interopérabilité, la mise en œuvre de deux nouvelles directives européennes et d'un règlement européen le 16 juin 2019 dans le cadre du « 4e paquet ferroviaire[5] » renforce le rôle de l'Agence de l'Union européenne pour les chemins de fer (ERA, acronyme anglais) qui délivre les autorisations internationales pour les matériels roulants et les certificats de sécurité internationaux pour les entreprises ferroviaires dans l'ensemble de l'Union européenne, en coopération avec les autorités nationales qui restent pleinement compétentes en matière de contrôle.

Le 4e paquet ferroviaire, constitué d'un ensemble de cinq textes européens au total composant le pilier « technique » (ERA, interopérabilité et sécurité ferroviaire) et le volet « marché » (gouvernance des acteurs et ouverture à la concurrence du transport de voyageurs) constitue l'étape la plus récente de la libéralisation du rail, initiée lors des paquets précédents.

---

[5] Voir https://www.ecologique-solidaire.gouv.fr/ouverture-concurrence-du-transport-ferroviaire-paquets-ferroviaires-et-creation-larafer qui explicite les différents paquets ferroviaires

De manière résumée et simplifiée, le système ferroviaire peut être décomposé en deux natures d'objets : les objets techniques (matériel roulant, infrastructure, signalisation) et les organisations, elles-mêmes s'appuyant sur les facteurs humains pour asseoir leur fonctionnement.

Chaque « objet » technique nouveau, qu'il s'agisse d'un train ou d'une infrastructure, doit faire l'objet d'une autorisation par l'autorité de sécurité compétente. Pour obtenir cette autorisation, le demandeur doit démontrer par un dossier de sécurité que l'objet en question est conforme aux règlementations européennes (appelées « spécifications techniques d'interopérabilité » - STI) et, le cas échéant, aux règles nationales (reflétant les spécificités techniques du réseau considéré).

Cette conformité réglementaire est obligatoire. Associée à une analyse des risques ferroviaires, elle constitue la base des démonstrations de sécurité. Ainsi, un train ou une infrastructure respectant les normes appelées par le cadre réglementaire sera réputé fonctionner en sécurité.

Les enjeux de sécurité devront ensuite être traités en exploitation et assurés également par la maintenance et l'entretien.

Deux acteurs majeurs interagissent sur les réseaux ferroviaires : les entreprises ferroviaires qui exploitent des services de transport de marchandises ou de voyageurs et les gestionnaires d'infrastructure en charge de la gestion des circulations et de la maintenance de leur réseau.

Comme pour les objets techniques, chaque exploitant doit être autorisé et contrôlé sur la base d'un système de gestion de la sécurité (SGS) démontrant sa capacité à identifier et traiter les risques ferroviaires liés à son activité (gestion documentaire, maintenance, gestion des compétences mais aussi diffusion d'une culture de sécurité au sein de l'entreprise et gestion des facteurs organisationnels et humains).

Le principe de base de la sécurité ferroviaire est qu'il est interdit de dégrader le niveau de sécurité global du système (par l'introduction de nouveaux items ou de changements de l'existant).

L'analyse des risques constitue le dénominateur commun entre les entités autorisées et les autorités de sécurité. C'est cette analyse qui va permettre d'identifier les risques puis de mettre en place des barrières de sécurité permettant de les couvrir.

Le cadre réglementaire européen est décrit dans le règlement d'exécution n° 402/2013 de la Commission européenne concernant la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques applicable dans le secteur ferroviaire. Il indique notamment trois principes d'acceptation des risques :

- **l'application de règles de l'art**, en premier lieu les spécifications réglementaires et les normes dont il est admis que leur respect garantit un niveau de sécurité acceptable ;
- **une comparaison avec un système similaire**, dans la mesure où ce système a démontré au travers de son fonctionnement qu'il garantit un niveau de sécurité acceptable ;
- **une estimation explicite des risques,** notamment appelée lorsque les deux premiers principes ne peuvent pas être utilisés, et qui fait appel aux techniques de sûreté de fonctionnement. Ce principe est particulièrement utilisé dans le cadre d'innovations disruptives pour lesquelles aucun cadre réglementaire n'est défini et qu'il n'existe aucun système similaire. L'introduction croissante de nouvelles technologies tend à augmenter l'utilisation de ce principe.

➔ **Cette réglementation ferroviaire ne prévoit pas, à ce jour, de dispositions spécifiques à la cybersécurité, ni d'interfaces avec les autorités et organismes compétents en la matière.**

1.2 Le cadre réglementaire en matière de cybersécurité

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale. Elle est rattachée au secrétaire général de la Défense et de la sécurité nationale, sous l'autorité du Premier ministre.

L'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité et de défense des systèmes d'information.

À ce titre :

- elle conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ;
- elle assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité et dans le cadre des orientations fixées par le Premier ministre, elle décide les mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne l'action gouvernementale ;
- elle anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;
- elle élabore les mesures de protection des systèmes d'information proposées au Premier ministre. Elle veille à l'application des mesures adoptées ;
- elle mène des inspections des systèmes d'information des services de l'État ;
- elle met en œuvre un système de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'État et coordonne la réaction à ces évènements ;
- elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information de l'État ;
- elle délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la Défense nationale ;
- elle participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;
- elle assure la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

L'Agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

L'agence est en particulier chargée, par délégation du Premier ministre :

- de la certification de sécurité des dispositifs de création et de vérification de signature électronique ;
- de l'agrément des centres d'évaluation et de la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

- de la délivrance des autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie.

L'Agence européenne chargée de la sécurité des réseaux et de l'information – ENISA selon l'acronyme en anglais – est une agence de l'Union européenne créée le 10 mars 2004 par un règlement de l'Union européenne.

À ce titre :

- elle conseille et assiste la Commission et les États membres en matière de sécurité de l'information et les aide, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle ;
- elle recueille et analyse les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents ;
- elle promeut des méthodes d'évaluation et de gestion des risques afin d'améliorer la capacité de faire face aux menaces pesant sur la sécurité de l'information ;
- elle favorise l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées ;
- elle suit l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

Le règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA – désormais Agence de l'Union européenne pour la cybersécurité – et à la certification de cybersécurité des technologies de l'information et des communications, vient renforcer son rôle et élargir ses missions. En effet, elle se voit dotée d'un mandat permanent ainsi que de ressources supplémentaires. Elle a également la responsabilité de développer un cadre de certification européen de cybersécurité pour les produits, les procédés et les services qui seront valables dans toute l'Union européenne.

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, l'ANSSI a pour mission d'accompagner les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information sensibles. La cybersécurité des OIV s'intègre dans le dispositif interministériel plus large de sécurité des activités d'importance vitale (SAIV) inscrit dans le code de la défense. Ces activités sont réparties par secteur d'activité rattaché à un ministère coordonnateur. Interlocuteur privilégié pour l'ensemble des enjeux « métier », le ministère est chargé d'apporter son expertise sur le secteur d'activité dont il a la charge. Ce dispositif a permis d'identifier les OIV, privés et publics, qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.

Pour faire face aux nouvelles menaces de nature « cyber », l'article 22 de la loi de programmation militaire (ou LPM, loi n° 2013-1168 du 18 décembre 2013), qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale de 2013, rajoute une pierre à l'édifice en imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV). Cette sécurisation passe notamment par l'application d'un certain nombre de règles de sécurité édictée par l'ANSSI, positionnée de ce fait dans un rôle de régulateur. Ils doivent notifier sans délai à l'ANSSI si un incident affecte le fonctionnement ou la sécurité d'un SIIV et ils peuvent être soumis à des contrôles. **Ce dispositif est pleinement effectif depuis octobre 2016 pour certains opérateurs du secteur ferroviaire.**

Adoptée le 6 juillet 2016, la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information, dite directive SRI ou *NIS* en anglais, a été transposée en 2018 dans le Droit national. Les opérateurs de service essentiel (OSE) au fonctionnement de l'économie et de la société sont tenus de sécuriser leurs systèmes d'information les plus sensibles en respectant des règles de sécurité édictées par l'ANSSI. Ils doivent notifier sans délai à l'ANSSI si un incident affecte le fonctionnement ou la sécurité de ces systèmes d'information et ils peuvent être soumis à des contrôles. **Ce dispositif est pleinement effectif depuis septembre 2018 pour certains opérateurs du secteur ferroviaire.**

Ces deux dispositifs visent à élever le niveau de cybersécurité des infrastructures critiques, notamment celles du transport ferroviaire. **Toutefois, la totalité des systèmes informatiques nécessaires au fonctionnement du système ferroviaire n'est pas concernée par ces réglementations qui se cantonnent aux infrastructures critiques.** De plus, les différentes approches retenues par les États membres ne concourent pas toujours à garantir un niveau équivalent et partagé entre les différents acteurs.

➔ **L'interopérabilité « cyber » n'est donc pas actuellement pleinement assurée à l'échelle européenne.**

2. Enjeux

2.1 Les travaux et initiatives en cours[6]

2.1.1. Dans le transport ferroviaire

Des initiatives diverses destinées à mieux cerner et cadrer la prise en compte de la cybersécurité dans le transport ferroviaire se sont multipliées ces deux dernières années. Ainsi que ce soit au niveau de la recherche, du champ normatif, du réglementaire, ou des partenariats, les acteurs concernés cherchent à se structurer afin de tenter d'articuler au mieux sécurité ferroviaire et cybersécurité et de renforcer, par là même, la prise en compte de la cybersécurité. Des conférences aux niveaux national et européen sont régulièrement organisées sur ce sujet.

S'il est difficilement possible d'être exhaustif en la matière, les initiatives suivantes peuvent être considérées comme notables.

- Au niveau national, l'EPSF et l'ANSSI ont signé, le 20 mars 2018, une lettre d'intention relative à la coopération dans le domaine de la sécurité des systèmes d'information. Concrètement, il s'agit pour les deux entités d'échanger des informations concernant des incidents affectant les systèmes d'information d'opérateurs relevant du domaine de compétence de l'EPSF, de travailler à l'identification et à l'articulation entre elles des exigences de sécurité ferroviaire et celles de la sécurité associée aux malveillances en ce qui concerne les équipements de communication et les logiciels (dont la présente note est un premier livrable), et de collaborer d'une manière générale dans le domaine de la sécurité des systèmes d'information (notamment par des actions de sensibilisation et de formation). Ce travail est très émergeant et vise notamment à aboutir à une vision française de ces sujets, avant de porter des positions partagées à l'échelle européenne, dans le cadre des révisions de la règlementation au mode d'adoption complexe, et faisant l'objet de divergences profondes entre les États sur le sujet de la cybersécurité.

  L'EPSF et l'ANSSI ont signé une lettre d'intention relative à la coopération dans le domaine de la sécurité des systèmes d'information.

- Depuis 2014, des chantiers conjoints sont menés entre la SNCF et l'ANSSI, encouragés par le corpus réglementaire cité précédemment (LPM / directive NIS). Ces travaux se matérialisent par de l'accompagnement technique et organisationnel, des audits et des partenariats plus formels autour de projets innovants tels que le train autonome.

- Les acteurs cherchent également à se fédérer. Ainsi, à l'initiative d'Infrabel (gestionnaire d'infrastructure belge), de DB Netz (gestionnaire d'infrastructure allemand) et avec le support de l'ENISA, plusieurs acteurs européens du secteur ferroviaire (gestionnaires d'infrastructure et entreprises ferroviaires de France, de Belgique, d'Allemagne, des Pays-Bas) ont initié en 2019 une plateforme d'échange à propos des risques cyber : ER-ISAC (*European Railway - Information Sharing and Analysis Center*). Le but de cette plateforme est de former un groupe de confiance capable de faire circuler des informations pertinentes sur les risques cyber en cours et sur le niveau de fiabilité de certains produits ou services et, de manière plus générale, d'assurer la promotion de cette thématique vers les acteurs

[6] L'approche ne se veut pas exhaustive

institutionnels. Les informations et bonnes pratiques en provenance de cette plateforme pourraient être considérées comme des contributions au cadre réglementaire ou à l'élaboration de normes. En plus des membres (des entreprises ferroviaires et des gestionnaires d'infrastructures européens), d'autres partenaires peuvent contribuer, tels que des industriels du domaine ferroviaire, des administrations nationales ou européennes dans le domaine de la cybersécurité ou du ferroviaire, des instituts de recherche et enfin d'autres ISAC.

- Dans le domaine de la recherche et de l'innovation, le partenariat public-privé européen Shift2Rail, qui a vocation à offrir une plateforme de collaboration pour la recherche et l'innovation pour l'espace ferroviaire européen unique, traite de la cybersécurité dans l'une de ses instances. Il s'agit notamment de mettre en place un démonstrateur technique spécifique visant à établir une analyse complète des risques de cybersécurité du système de contrôle-commande ERTMS, des mesures de protection pour chaque sous-système, ainsi qu'une architecture appropriée (établissant notamment des zones à niveaux de sécurité différenciés). Différents acteurs du secteur ferroviaire (constructeurs, équipementiers, exploitants, etc.) sont représentés dans le groupe de travail et des discussions sont en cours avec l'Agence de l'Union européenne pour les chemins de fer pour refléter, dans les futures versions des spécifications techniques d'interopérabilité, les besoins d'harmonisation de certaines interfaces assurant l'interopérabilité : interface radio, chiffrement des messages de signalisation ETCS, etc.

- Au niveau normatif, le groupe de travail CEN/CENELEC dédié à la sécurité des systèmes d'information et à la cybersécurité (WG 26) vise à établir une spécification technique européenne (TS 50701) relative à la cybersécurité appliquée au secteur ferroviaire, spécification appelée à terme à devenir une norme. Les travaux s'appuient sur la norme internationale IEC 62443 - « Cyber-sécurité des installations industrielles ». Le groupe de travail rassemble les acteurs majeurs du secteur ferroviaire (constructeurs, équipementiers, exploitants). Cette spécification proposera notamment des modèles d'architecture, les grands principes d'évaluation des risques de cybersécurité, des jeux de mesures de cybersécurité applicables par zone de criticité cyber, et les activités de cybersécurité durant la durée de vie du produit (cf. §2.2.2 Maintien en condition de sécurité). Cette future norme, qui pourrait servir de recommandation pour inciter les opérateurs et les industriels à se pencher avec plus de précision sur la question de la cybersécurité, est encore en phase de revue.

- L'Union internationale des chemins de fer (UIC) développe des spécifications de télécommunication ferroviaire, et notamment un programme pour le successeur de la radio sol-bord GSM-R intitulé *Future Railway Mobile Communication System* (FRMCS). Ce nouveau système de télécommunication devrait se reposer sur la norme de téléphonie 5G et intégrer nativement des éléments de protection contre les menaces cyber en comparaison des possibilités offertes par les anciens systèmes de télécommunication. La télécommunication étant un levier majeur pour la numérisation des technologies ferroviaires, les mesures de protection de celle-ci seront essentielles.

2.1.2. Exemple de fonctionnement dans d'autres secteurs

Il paraît difficile d'être exhaustif tant les secteurs concernés par la cybersécurité sont variés et la maturité face aux risques de cybersécurité n'est pas identique dans tous les secteurs d'activité.

Le transport aérien s'est rapidement intéressé à ce sujet. Cela s'explique sans doute par l'existence d'une culture fortement axée sur la sécurité et la sûreté, par l'organisation du secteur efficace dès les premiers développements du transport international qui permet une homogénéité des pratiques et un travail en commun efficace au niveau mondial.

Aujourd'hui, au niveau européen, l'Agence de l'Union européenne pour la sécurité aérienne a pour mission de coordonner globalement les problématiques cyber pour le secteur de l'aviation. En collaboration avec tous les acteurs du secteur, elle veille à ce que les risques cyber pour les systèmes européens de navigation aérienne soient pris en considération durant la phase de conception et de maintien en conditions opérationnelles. Pour atteindre ces objectifs, elle organise régulièrement des ateliers pour renforcer la coopération, pour inclure la cybersécurité dans le concept de sécurité aérienne.

En France, la création récente d'un Conseil pour la cybersécurité du transport aérien (CCTA) sous l'égide de la DGAC, instance de coordination des services de l'État, des constructeurs, des équipementiers, des exploitants et des fédérations professionnelles de l'aviation civile, vise à encadrer, structurer et coordonner les initiatives concernant la cybersécurité du secteur aérien français, et à porter la voix de la France dans les groupes de travail techniques européens et internationaux.

Le Conseil, est organisé autour de trois comités techniques :

- CT1 : « risques cyber », chargé de tenir à jour une hiérarchie des risques pouvant affecter la filière du transport aérien ;
- CT2 : « impact », chargé de proposer des mesures d'atténuation de ces risques, en tenant compte de l'impact de ces mesures (sûreté, économie, etc.) ;
- CT3 : « réglementation », chargé de formuler des projets de textes nationaux et déployer une stratégie d'influence auprès des instances internationales.

Une initiative similaire a été lancée dans le secteur automobile en mai 2019 avec le CSTA30.

L'ENISA a organisé, en janvier 2019 à Lisbonne, la première conférence sur la cybersécurité dans les transports avec le soutien de la Commission européenne, de l'Agence européenne de la sécurité aérienne, de l'Agence européenne pour la sécurité maritime et de l'Agence de l'Union européenne pour les chemins de fer. Cet événement marque la prise en compte du sujet de la cybersécurité au plus haut niveau et ouvre de nouvelles perspectives quant à la relation entre la sécurité des activités de transport et la cybersécurité. À terme, cette réflexion devrait aussi contribuer à l'élaboration du cadre de certification cyber porté par l'ENISA pour les aspects spécifiques au transport.

2.2 Sécurité ferroviaire et cybersécurité : une frontière poreuse

2.2.1. Nouvelles technologies, nouvelles connectivités, nouveaux risques

Les systèmes d'informations industriels ferroviaires, qu'ils soient de maintenance ou de contrôle-commande, au sol comme à bord, sont de plus en plus informatisés. À ceux-ci s'ajoutent de nombreux systèmes de confort ou de divertissement embarqués dont la vocation est d'améliorer l'expérience de voyage pour les clients.

Tous mettent désormais en œuvre des technologies de plus en plus standardisées issues du monde de l'informatique traditionnelle ; là où, par le passé, les systèmes étaient généralement propriétaires et spécifiques. Ainsi, réseaux IP et distributions logicielles non spécifiques ont désormais une place importante à bord des trains et sur les infrastructures au sol.

Cette situation est duale ; elle facilite les évolutions fonctionnelles (connectivités plus faciles à envisager) et la prise en compte de la cybersécurité (technologies bénéficiant d'une communauté utilisateurs, produits de cybersécurité disponibles sur le marché) ; mais elle entraîne aussi une augmentation de la probabilité d'attaques informatiques malveillantes (protocoles et couches logicielles standard, vulnérabilités publiques).

Pour faire face à cette situation, un certain nombre de points sensibles (voir ci-après) sont à mettre sous contrôle d'un point de vue cybersécurité ; plus particulièrement sur les SI industriels qui peuvent contribuer à la sûreté de fonctionnement du système ferroviaire.

- **Les accès pour la maintenance** :

  À la première place des connectivités à mettre sous contrôle, il y a celle relative aux accès physiques, et notamment celles du mainteneur (opérations de relève de défauts, visualisation) et de l'administrateur du système (opérations de reprogrammation et paramétrages avancés).

  Il y a un enjeu fort de maîtrise des appareillages connectés (postes informatiques et outillages), des accès aux données (principe des moindres privilèges) surtout si celles-ci contiennent des secrets logiciels, des données personnelles ou des journaux d'opérations réalisées (traçabilité) notamment lorsqu'il s'agit de programmation ou paramétrage.

  L'usage de terminaux mobiles accroît la sensibilité ; en effet la cybersécurité d'un terminal nomade est par défaut difficilement maîtrisable, l'accès via ces terminaux nomades augmente le risque de compromission et offre ainsi une porte d'entrée potentielle à un attaquant.

  La maîtrise de ces enjeux passe par des mesures techniques (durcissement, cloisonnement, gestion des droits, etc.) et organisationnelles (sensibilisation, formation, etc.).

  La télémaintenance et autres téléopérations (parfois externalisées), qui s'appuient sur des objets connectés en cours de déploiement massif sur le réseau ferré, sont à classer dans cette catégorie, avec la mise en place de liens bord/sol (autrement dit entre le matériel roulant et le sol), et la mise en place de capteurs positionnés sur les SI industriels.

  L'accès à distance augmente considérablement la surface d'attaque d'un système.

La couverture des risques inhérents à ces déploiements s'appuie sur une combinaison de mesures techniques (cloisonnement, authentification, chiffrement, etc.) et organisationnelles (contractualisation sécurité avec les partenaires, etc.).

En complément des vulnérabilités applicatives, les vulnérabilités des couches basses (électroniques, firmwares, etc.) seront à considérer dans les prochaines années. Le binôme protection physique et logique sera alors essentiel pour maîtriser les risques associés.

❖ **Le déploiement de connectivités sans-fil** :

En plein essor, la connectivité sans-fil entre les composants informatiques est en train de s'imposer au fonctionnement du système ferroviaire, par les possibilités qu'elle offre en matière de diagnostic à distance, de géolocalisation ou encore de collecte de données utiles à la maintenance. De même, l'amélioration de l'« expérience client » passe par ces nouveaux usages (information voyageurs temps réel, Internet à bord, etc.). Sur ces liens particulièrement exposés, les mesures de cybersécurité sont essentielles ; d'autant que des flux critiques peuvent y transiter, comme des informations de signalisation, de pilotage ou encore des fonctionnalités de programmation à distance.

Encouragées par la numérisation et l'hyperconnectivité de la société, les interactions entre les trains et les clients se développent et induisent également une surface d'exposition aux cyberattaques accrue.

Dans ces cas, la protection physique des systèmes et réseaux (première barrière de défense des systèmes ferroviaires) est inefficace. Il est primordial d'envisager une cybersécurité intégrée au système *by design* pour répondre à ces enjeux. Cloisonnement, filtrage, authentification, surveillance et journalisation sont autant de mesures nécessaires à la bonne tenue en service de telles solutions.

➔ **L'ensemble de ces aspects ne fait pas l'objet d'une évaluation dans le cadre de la délivrance des autorisations des exploitants ferroviaires car non intégrés dans la règlementation relative aux systèmes de gestion de la sécurité ferroviaire.**

Bien qu'intrinsèquement conçus pour réagir fonctionnellement dans des modes de repli compatibles avec la sécurité (au sens de la sécurité ferroviaire), **les SI industriels portant des fonctions de sécurité ne peuvent plus faire abstraction de la cybersécurité.**

Comme évoqué, l'emploi de nouvelles technologies laissant une large place au numérique, l'augmentation des surfaces d'attaques qu'elles génèrent met en évidence le **besoin impérieux d'articuler plus intimement sécurité ferroviaire et cybersécurité**. **Au-delà de ces aspects, la tenue des objectifs de disponibilité** (le repli d'un système étant souvent synonyme d'indisponibilité) **est également un enjeu fort** pour les exploitants sujets à un évènement de sécurité.

2.2.2. Deux logiques antagonistes : la démonstration de sécurité ferroviaire (safety) et le maintien en condition de sécurité (cyber)

La réglementation ferroviaire impose à tout système informatique embarqué dans un matériel roulant ou équipant une infrastructure (contrôle-commande et signalisation) la réalisation d'une analyse qui, selon son importance, peut donner lieu à une autorisation de la part de l'autorité de sécurité. Chaque évolution d'un système existant (évolution matérielle ou logicielle) passe par ce type d'analyse qui doit être tracée et adjointe au dossier technique du système considéré. Dans le cas d'évolution logicielle, souvent jugée comme ne nécessitant pas de nouvelle autorisation, l'analyse nécessite souvent plusieurs jours à plusieurs semaines afin de s'assurer de la non-régression du système mis à jour, autrement dit que celle-ci ne vienne pas engendrer des dysfonctionnements préjudiciables à la sécurité. La traçabilité est primordiale, notamment pour la prise en compte du critère d'additionnalité (plusieurs mises à jour mineures successives peuvent constituer un changement important pour la sécurité à terme).

Le maintien en condition de sécurité (dit « MCS ») définit quant à lui l'ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de cybersécurité tout au long du cycle de vie d'un système. Notamment, il s'appuie sur :

- une maitrise de la cartographie (technique, physique) des composants matériels et logiciels et des processus organisationnels afférents ;
- une veille des vulnérabilités sur ceux-ci ;
- un traitement de celles-ci via des correctifs ou des mesures de contournement (techniques ou organisationnelles) permettant de maintenir le niveau de cybersécurité dans le temps.

Le « temps ferroviaire » (temps d'analyse et de tests de non-régression) et le « temps cyber » sont asynchrones :

- un système dans sa version autorisée par l'autorité de sécurité reste sûr s'agissant de la sécurité ferroviaire tout le long de son cycle de vie (entre 15 et 25 ans) tant qu'il n'évolue pas de manière importante. Mais chaque modification, même mineure, doit faire l'objet d'une analyse ;
- le même système cyber-sécurisé dans sa version à un jour J peut devenir non cyber-sécurisé au jour J+1, et doit donc être maintenu en sécurité en permanence (par l'application de correctifs notamment), ce qui apparaît difficilement compatible avec le temps d'analyser l'impact de la modification sur la sécurité ferroviaire.

L'enjeu principal est donc de réussir à définir des processus permettant un MCS agile et raisonné au service d'un système de sécurité ferroviaire qui reste conforme aux termes par lesquels il a été autorisé.

2.2.3. Les exigences en matière de cybersécurité vont-elles durcir les conditions d'admission[7] des matériels roulants sur les infrastructures ?

En sécurité ferroviaire, tout train préalablement autorisé doit faire l'objet d'une vérification de sa compatibilité avec l'infrastructure sur laquelle il sera amené à circuler. Cette vérification est due aux spécificités historiques des réseaux nationaux (caractéristiques de voies, de signalisation, de caténaires, etc.) qui imposent ces vérifications aux matériels, mêmes si ceux-ci sont conformes à la règlementation en vigueur.

Les spécifications techniques d'interopérabilité gomment progressivement ces spécificités, au fur et à mesure que les lignes considérées sont renouvelées ou réaménagées. Pour effectuer cette vérification, qui incombe aux entreprises ferroviaires, chaque gestionnaire d'infrastructure a l'obligation de publier un registre de l'infrastructure, décrivant les caractéristiques de son réseau. Ce registre est harmonisé à l'échelle européenne.

Il n'y a, à ce jour, aucun critère en lien avec la cybersécurité dans le processus de vérification de compatibilité : un gestionnaire d'infrastructure ne peut donc pas imposer d'exigences de nature cybersécurité, même s'il estime que la circulation d'un train pourrait constituer une menace en termes de cyberattaque.

Les angles d'attaques potentiels peuvent être multidirectionnels : d'un train vers l'infrastructure, d'une infrastructure vers un train, mais aussi entre deux trains ou deux infrastructures exploités par des opérateurs différents.

L'introduction d'exigences potentiellement très différentes et divergentes par les gestionnaires d'infrastructure pour admettre les trains sur leur réseau aurait un effet négatif sur l'interopérabilité ferroviaire. Inversement, quelles garanties ont les opérateurs que l'infrastructure ne constituera pas un vecteur d'attaque envers leur matériel roulant ?

2.2.4. Les enjeux de disponibilités du système ferroviaire

Les processus concourant à la sécurité de l'exploitation ferroviaire ont longtemps reposé sur un triptyque « humain – organisation - procédés techniques indépendants des systèmes d'information ».

Depuis plusieurs années, encouragés par la transformation numérique du secteur, et par les opportunités fonctionnelles offertes, ces processus s'appuient de plus en plus sur des systèmes d'information ; créant ainsi une « SI dépendance ».

Dans le cas d'une malveillance dirigée contre un système d'information assujetti à ces dépendances, tout ou partie de l'exploitation pourrait être dégradée ou interrompue.

[7] Par admission, il faut comprendre démarche globale de mise en exploitation d'un train sur une infrastructure (autorisation, vérification de compatibilité, …)

Un déni de service sur ces systèmes d'information impacterait directement la capacité d'exploitation du système ferroviaire.

La démarche de maîtrise de la sûreté de fonctionnement, notamment pour les systèmes assurant des fonctions de sécurité, implique des états déterministes et des modes dégradés prévus.

Dans le cas d'une malveillance conduisant le système dans un état non prévu, le mode de repli mis en œuvre sera en général l'arrêt du système (ex : freinage d'urgence, signalisation fermée, etc.).

Dans cette logique de robustesse via basculement en mode de repli permettant de garantir la maîtrise de la sûreté de fonctionnement, une cyberattaque pourrait aisément provoquer une indisponibilité du système.

3. Recommandations (actions et méthodes de mise en œuvre)

Compte tenu des constats évoqués dans la présente note, il conviendrait d'adopter une approche convergente (technique et réglementaire) pour garantir la sécurité des systèmes ferroviaires, autant au sens de la sûreté de fonctionnement qu'au sens de la disponibilité et de l'intégrité des systèmes d'information.

À ce stade des réflexions, plusieurs recommandations peuvent être émises :

Recommandation R1 : Accentuer la coopération entre l'EPSF et l'ANSSI pour tendre vers une position française sur l'articulation entre sécurité ferroviaire et cybersécurité

La lettre d'intention signée entre l'EPSF et l'ANSSI en 2018 a permis d'initier un dialogue entre les deux autorités dont la présente note constitue un premier résultat concret, en association avec SNCF et l'ERA.

Sur la base de cette note, il s'agit de bâtir une position « française » sur les sujets mis en exergue qui constituerait une feuille de route pouvant être portée de manière coordonnée au sein des instances européennes dans le cadre des réglementations à venir.

Le présent travail pourrait être approfondi sur la question des moyens, des compétences, des processus à mettre en place pour porter un schéma clair et inclusif des questions liées à la sécurité, qu'elle soit ferroviaire ou cyber.

Il s'agira également de prioriser les enjeux : systèmes existants, innovations faisant largement appel au numérique, adéquation des moyens des acteurs par rapport à leur exposition au risque, etc.

Enfin, l'accentuation du partage autour des évènements de sécurité et des analyses des risques associées, éventuellement sur des cas simulés de cyberattaques ferroviaires, permettrait de tester les schémas proposés.

***

Recommandation R2 : Disposer d'un panorama européen sur l'articulation cybersécurité et sécurité ferroviaire

---

Portée par l'ERA en coordination avec l'ENISA, il s'agirait d'obtenir un panorama européen des positions des États membres sur les sujets évoqués dans cette note, voire d'identifier d'autres sujets qui préoccuperaient nos homologues.

Ce panorama servirait de donnée d'entrée pour la préparation d'un futur cadre réglementaire européen harmonisé et convergeant dans la prise en compte de la cybersécurité ferroviaire, à définir les rôles futurs des organismes d'évaluation et des

autorités de sécurité quant aux certifications, autorisations, voire simples déclarations des acteurs à délivrer, et de préciser les périmètres de responsabilité de chacun.

Il s'agirait également de mieux connaître la feuille de route de l'ENISA et la nature des relations et la répartition des actions entre l'ERA et l'ENISA.

***

Recommandation R3 : Favoriser le partage d'informations et coordonner les actions de la filière ferroviaire française sur la cybersécurité

Depuis quelques années, face à l'augmentation de la cybermenace, la France s'est dotée d'un dispositif réglementaire qui répond partiellement aux besoins de sécurité puisque sa portée reste insuffisante (voir §1.2). Le sujet de la cybersécurité prenant toujours plus d'importance, de nombreux lieux d'échanges se sont constitués où différentes visions s'affrontent. Ces visions sont insuffisamment partagées. Le développement et le déploiement accrus de nouvelles technologies numériques pourraient être freinés en cas d'évènement impactant la sécurité globale du système.

En outre, le système ferroviaire vise l'interopérabilité de ses réseaux et des matériels qui y circulent. Les contraintes liées à la protection en matière de cybersécurité peuvent entraver cette interopérabilité (voir §2.2.3) en introduisant des critères pouvant restreindre les possibilités de circulation. Une approche « globale » de ces contraintes renforce la nécessité de coordonner l'ensemble des acteurs concernés.

Aussi, la création d'une enceinte dédiée à la cybersécurité du secteur ferroviaire, regroupant l'ensemble des parties prenantes (institutionnels, industriels, équipementiers, exploitants, fédérations) à l'image du CCTA aérien, permettrait de mieux structurer la filière, d'aborder les problématiques « système » pour y apporter des solutions concertées et contribuerait à synchroniser les positions à défendre au niveau européen ou international.

***

Recommandation R4 : Intégrer la dimension cybersécurité dès le début des projets

---

La prise en compte étroite de la cybersécurité est essentielle afin de garantir un niveau de sécurité acceptable lors des mises en service, puis tout au long du cycle de vie.

Aussi, il apparait pertinent :

– d'intégrer la cybersécurité dès l'émergence des projets (dans les spécifications, dans les choix technologiques et d'architecture) ceci afin de réduire les coûts de la cybersécurité et faciliter le travail d'intégration ;
– de standardiser et systématiser la démarche relative à la cybersécurité au sein des organisations afin d'avoir une cohérence globale ;

– de maintenir à jour une macro-cartographie des risques de cybersécurité issue de ces accompagnements.

Cette recommandation concerne l'ensemble des parties prenantes (opérateurs et industriels) en charge de la conception ou de la modification de composants unitaires ou de systèmes complexes.

***

Recommandation R5 : Mettre en œuvre un maintien en condition de sécurité (MCS) raisonné tout en réduisant au maximum les impacts sur les démonstrations de sécurité (au sens de la sûreté de fonctionnement)

Le paragraphe 2.2.2 de la présente note met en lumière les divergences de temporalités entre cybersécurité (MCS nécessitant une rapidité d'exécution) et sûreté de fonctionnement (démonstration de sécurité stabilisée).

L'approche pour accorder le MCS et la démonstration de sécurité pourrait reposer sur les éléments suivants :

– adopter une approche « sécurité dès la conception » (*secure by design*) pour la définition de l'architecture réseau du train : conception faisant appel à des briques modulaires visant à séparer les briques SSI de la couche applicative ; et défense en profondeur efficace sur les chemins d'attaques les plus sensibles ;

– définir un périmètre sur lequel le MCS se veut prioritaire, en effectuant un inventaire des composants jugés les plus critiques au regard du MCS global du système (équipements assurant des fonctions de cybersécurité, systèmes en interactions directes avec de potentiels accès illégitimes) ;

– définir des règles d'application en amont : stratégie de MCS générique et déclinaison par système selon les spécificités de celui-ci (architectures, technologies, composants, expositions, etc.) permettant de cadrer la veille aux vulnérabilités, le calcul contextualisé de leur criticité, le modèle de décision pour le déploiement ;

– contractualiser les activités de MCS avec les industriels pour les produits spécifiques (bulletins de vulnérabilités et fourniture de patchs correctifs / mesures de contournement) ;

– mettre en œuvre des plateformes de tests et recettes.

Ce type d'approche serait à partager avec l'ensemble des acteurs du secteur ferroviaire, et sur la base d'un consensus, être décliné au niveau de guides ou normes sectorielles.

***

Recommandation R6 : Identifier les répercussions que la cybersécurité pourrait avoir sur l'interopérabilité dans un secteur avec un nombre d'acteurs et un trafic transfrontalier en croissance

---

Le paragraphe 2.2.3 de la présente note met en lumière la possible apparition prochaine de contraintes liées à des exigences de cybersécurité qui seraient différentes selon les exploitants. Une telle situation impacterait l'ensemble des exploitants à leurs interfaces et notamment l'admission croisée entre le matériel roulant et l'infrastructure.

Pour éviter un tel obstacle, il serait judicieux :

- d'identifier les technologies / systèmes / interfaces pouvant conduire à terme à une telle situation et analyser les risques induits par ces interfaces. De rechercher si, pour les cas identifiés, des technologies seraient disponibles afin de permettre à un opérateur de protéger ses propres interfaces sans impacter les parties prenantes avec des contraintes exportées ;
- d'évaluer si, pour les cas identifiés, des spécifications communes permettraient de standardiser ces interfaces avec un niveau de sécurité suffisant et/ou démontrable (spécification technique d'interopérabilité, norme, etc.) ;
- d'identifier si, pour les cas identifiés, la démarche de certification en cours d'instruction au niveau européen pourrait être une réponse à l'amortissement de contraintes exportées.

Les parties prenantes (industriels, équipementiers, organismes de certification …) pourraient apporter leur contribution à cette démarche de standardisation / certification, afin de concourir à la réalisation du marché unique des services de transport ferroviaire.

***

Recommandation R7 : Accroître la robustesse des systèmes d'information essentiels à l'exploitation du système ferroviaire face à la menace de nature « cyber »

Le paragraphe 2.2.4 de la présente note met en lumière une dépendance croissante aux systèmes d'information pour assurer l'exploitation du système ferroviaire. Au-delà du périmètre lié à la sécurité ferroviaire, il convient de garantir la disponibilité des systèmes d'information qui concourent également au fonctionnement de l'exploitation.

Pour rendre le système plus résilient dans son ensemble, il apparaît nécessaire :

- de concevoir les systèmes d'information et les dépendances qui les relient, en les préservant des risques d'attaques de type déni de service ;
- dans le cas où un acte malveillant aurait abouti avec succès, d'anticiper les actions à mener au travers de :

- plans de continuité d’activités (ou « comment puis-je continuer à opérer sans mon système d’information, ou avec un système d’information dégradé ? »),
- plans de reprise d’activités (ou « comment puis-je remettre efficacement et rapidement mon système d’information en service nominal ? »).

Établissement public de sécurité ferroviaire

60, rue de la Vallée – CS 11758 – 80017 Amiens Cedex 1